

# NAVAL POSTGRADUATE SCHOOL

## Monterey, California



## THESIS

### PRELIMINARY ROADMAP FOR THE UNITED STATES MARINE CORPS PUBLIC KEY INFRASTRUCTURE

by

Dan E. Morris and David W. Rowe

September 1999

Thesis Advisor:  
Co-Advisor:  
Associate Advisor:

Cynthia Irvine  
Daniel Warren  
Terrance Brady

Approved for public release; distribution is unlimited.

# REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE

September 1999

3. REPORT TYPE AND DATES COVERED

Master's Thesis

4. TITLE AND SUBTITLE

Preliminary Roadmap for the United States Marine Corps Public Key Infrastructure

5. FUNDING NUMBERS

6. AUTHOR(S)

Morris, Dan E. and Rowe, David W.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School  
Monterey, CA 93943-5000

8. PERFORMING  
ORGANIZATION REPORT  
NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSORING /  
MONITORING  
AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

## 13. ABSTRACT

Over the last decade, the Marine Corps has capitalized on the advantages of the Internet by increasingly using the NIPRNET for electronic operations and communications. The Marine Corps wants to further leverage the capabilities of the Internet by moving more applications to the NIPRNET, however, security threats have restricted the type of information that can be exchanged across public networks. The Internet's open design enables message interception, monitoring and forgery; therefore, the Marine Corps is reluctant to use the Internet for transmitting sensitive information. Public key cryptography is becoming the foundation for electronic operations that require security and authentication in open networks. The use of public key cryptography requires a Public Key Infrastructure (PKI) to publish and manage public key values. The objective of a PKI is to provide authentication, confidentiality, integrity and non-repudiation of data. In conjunction with DoD PKI development efforts, the Marine Corps will develop and implement PKI services to protected information currently exchanged across the Internet and to enable the use of automated applications. This thesis begins by describing public key cryptography, the requirements for a PKI, and the components necessary to operate a PKI. Next, a preliminary USMC PKI roadmap is developed, including objectives and strategies for Marine Corps implementation efforts. Supporting material describes design issues, such as scalability and interoperability, and technical challenges, such as directories, key escrow, and smart cards. Finally, change management approaches are discussed, emphasizing unique cultural and organizational requirements for mitigating resistance to a Marine Corps PKI implementation.

14. SUBJECT TERMS

PKI, Public Key Infrastructures, Computer Security, MCEN, Marine Corps Enterprise Network

15. NUMBER OF  
PAGES

141

16. PRICE CODE

17. SECURITY CLASSIFICATION OF  
REPORT

Unclassified

18. SECURITY CLASSIFICATION OF  
THIS PAGE

Unclassified

19. SECURITY CLASSIFI- CATION  
OF ABSTRACT

Unclassified

20. LIMITATION  
OF ABSTRACT

UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)

Prescribed by ANSI Std. Z39-18 298-102



Approved for public release; distribution is unlimited.

**PRELIMINARY ROADMAP FOR THE UNITED STATES MARINE  
CORPS PUBLIC KEY INFRASTRUCTURE**

Dan E. Morris  
Major, United States Marine Corps  
B.S., Oklahoma State University, 1989

David W. Rowe  
Captain, United States Marine Corps  
B.A., Northwestern University, 1990

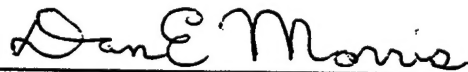
Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 1999**

Authors:

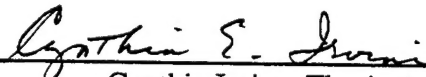


Dan E. Morris



David W. Rowe

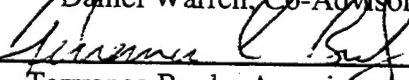
Approved by:



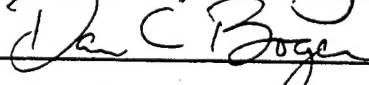
Cynthia Irvine, Thesis Advisor



Daniel Warren, Co-Advisor



Terrance Brady, Associate Advisor



Dan Boger, Chairman  
Information Systems Academic Group





## ABSTRACT

Over the last decade, the Marine Corps has capitalized on the advantages of the Internet by increasingly using the NIPRNET for electronic operations and communications. The Marine Corps wants to further leverage the capabilities of the Internet by moving more applications to the NIPRNET, however, security threats have restricted the type of information that can be exchanged across public networks. The Internet's open design enables message interception, monitoring and forgery; therefore, the Marine Corps is reluctant to use the Internet for transmitting sensitive information. Public key cryptography is becoming the foundation for electronic operations that require security and authentication in open networks. The use of public key cryptography requires a Public Key Infrastructure (PKI) to publish and manage public key values. The objective of a PKI is to provide authentication, confidentiality, integrity and non-repudiation of data. In conjunction with DoD PKI development efforts, the Marine Corps will develop and implement PKI services to protected information currently exchanged across the Internet and to enable the use of automated applications. This thesis begins by describing public key cryptography, the requirements for a PKI, and the components necessary to operate a PKI. Next, a preliminary USMC PKI roadmap is developed, including objectives and strategies for Marine Corps implementation efforts. Supporting material describes design issues, such as scalability and interoperability, and technical challenges, such as directories, key escrow, and smart cards. Finally, change management approaches are discussed, emphasizing unique cultural and organizational requirements for mitigating resistance to a Marine Corps PKI implementation.



# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>II.</b>	<b>PUBLIC KEY CRYPTOGRAPY AND INFRASTRUCTURES.....</b>	<b>11</b>
A.	SYMMETRIC CRYPTOGRAPHY .....	12
B.	CONFIDENTIALITY .....	15
C.	AUTHENTICATION AND INTEGRITY .....	17
D.	ESTABLISHING TRUST.....	20
E.	PUBLIC KEY INFRASTRUCTURES .....	22
1.	<i>PKI Elements</i> .....	23
2.	<i>PKI Hierarchy</i> .....	28
3.	<i>Certificate Generation and Distribution</i> .....	28
F.	CONCLUSION .....	33
<b>III.</b>	<b>USMC PKI ROLES, RESPONSIBILITIES AND OBJECTIVES.....</b>	<b>35</b>
A.	INTRODUCTION.....	35
B.	INFORMATION ASSURANCE AND THE DOD PKI.....	36
1.	<i>Achieving Information Assurance</i> .....	36
2.	<i>DoD PKI Structure</i> .....	37
3.	<i>Assurance Levels and Certificate Types</i> .....	41
C.	MARINE CORPS ROLES AND RESPONSIBILITIES .....	42
D.	USMC PKI OBJECTIVES.....	45
1.	<i>Certificate Management</i> .....	45
2.	<i>Registration</i> .....	47
3.	<i>Local Directories</i> .....	50
4.	<i>Applications</i> .....	51
E.	USMC PKI DEVELOPMENT RISKS AND INITIAL STRATEGY .....	52
F.	USMC DEVELOPMENT PROCESS .....	54
1.	<i>Conduct a USMC-Wide Survey</i> .....	54
2.	<i>Develop a Basic Design</i> .....	55
3.	<i>Evaluate Options</i> .....	56
4.	<i>Source and Deploy Infrastructure Components</i> .....	56
5.	<i>Re-Evaluate PKI Solutions</i> .....	57
G.	CONCLUSION .....	57
<b>IV.</b>	<b>TECHNICAL CHALLENGES .....</b>	<b>59</b>
A.	INTRODUCTION .....	59
B.	DIRECTORIES .....	60
1.	<i>Definition of a Directory</i> .....	60
2.	<i>Purposes of Directories</i> .....	60
3.	<i>Approaches to Directory Service Standards</i> .....	64
4.	<i>Directory Service Technology</i> .....	64
5.	<i>Metadirectories</i> .....	70
6.	<i>Recommendations</i> .....	72
C.	APPLICATIONS .....	81
D.	KEY ESCROW .....	82
1.	<i>Definition</i> .....	82
2.	<i>Issues</i> .....	83
3.	<i>Mechanics</i> .....	85
E.	SMART CARDS .....	88
F.	CONCLUSION .....	90

<b>V. CHANGE MANAGEMENT .....</b>	<b>91</b>
A. INTRODUCTION.....	91
1. <i>Purpose of Chapter</i> .....	91
2. <i>Definition of Change</i> .....	92
3. <i>Developing Strategies for Change</i> .....	93
B. CATEGORIZING CHANGE .....	95
1. <i>The Vision for Change</i> .....	95
2. <i>Strategic Choices for Enabling Change</i> .....	98
C. CHANGING THE CULTURE.....	104
1. <i>Overcoming Resistance to Change</i> .....	104
2. <i>Education and Training</i> .....	106
3. <i>Centralization of Procurement</i> .....	108
D. SUMMARY .....	110
<b>VI. CONCLUSION.....</b>	<b>113</b>
<b>LIST OF REFERENCES .....</b>	<b>121</b>
<b>BIBLIOGRAPHY .....</b>	<b>125</b>
<b>INITIAL DISTRIBUTION LIST .....</b>	<b>127</b>

## LIST OF FIGURES

Figure 1-1. Defense in Depth Concept.....	5
Figure 2-1. Symmetric Key Encryption .....	13
Figure 2-2. Public Key Encryption for Confidentiality.....	16
Figure 2-3. Basic Authentication with Public Key Pairs.....	18
Figure 2-4. Digital Signature Generation and Verification.....	20
Figure 2-5. PKI Hierarchical Structure .....	29
Figure 3-1. DoD PKI Organizational Levels (NIPRNET) .....	38
Figure 3-2. DoD Target User Registration (USMC).....	48
Figure 5-1. Progressions of Change Adoption .....	106



## I. INTRODUCTION

Paralleling the explosive growth of the Internet is the emergence of electronic operations as efficient, convenient, and cost-effective methods of conducting business transactions and exchanging information within and between organizations. For many organizations, electronic operations are much more than new and effective means of conducting business – they are vital components of daily operations and increasingly necessary ingredients for the survival of any organization hoping to compete in the lightning-fast environment of an information-based, network-centric economy and society. However, as organizations rely more and more on network-based applications, they are also struggling with the problem of how to conduct mission-critical operations over inadequately protected corporate intranets and extranets, as well as the publicly-accessed Internet. Network security architectures must be designed and integrated with existing network architectures to provide comprehensive protection from a growing number of network-based threats.

Public key infrastructures (PKI) are being deployed throughout private industry and the public sector to enable and support the utilization of public key cryptography. Although the technology for public key cryptography has been understood for over two decades, deploying the technology can be very difficult without a robust infrastructure to support it [Des97]. Despite years of research demonstrating that the integration of public key cryptography into existing network security strategies can significantly improve the overall security stature of computer networks, only within the last few years have PKIs



surfaced to provide the necessary structure and assurances required to fully and safely deploy public key systems and applications. The transition of the world economy from industry-based to information-based has rapidly accelerated the requirement for an infrastructure to support the services offered by public key cryptography. As a result, PKI is on the brink of wide scale deployment throughout the networked world to address a growing number and type of threats to network-based electronic operations.

Modern network security threats come in many different varieties, employing varying levels of sophistication. The conventional use of the term "hacker" invokes images ranging from a high school student breaking into systems for fun; a disgruntled employee seeking "revenge" by destroying company data; or even an international spy attempting to steal business or military secrets. These threats are still very real today and traditionally involve the act of "breaking into" an organization's private, internal networks and applications. However, the increasing use of the Internet and corporate-intranets to conduct core operations has led to the evolution of a more modern type of "hacker" or, more appropriately, *information criminal*. Information criminals include white-collar criminals, international spies, terrorist organizations, and even foreign intelligence organizations. They can intercept information as it travels within and between networks, and subsequently read, modify, or delete it to serve their individual interests. These "interests" may include embezzlement, fraud, corporate or military espionage, and electronic terrorism or vandalism. Information criminals may also electronically impersonate trading partners, trusted organizations, or even allied

government and military organizations to obtain information or send false or misleading information. Many information crimes are yet to be invented.

As a result of these threats, organizations must implement network boundary security systems designed to isolate their internal networks from public networks such as the Internet. They must also implement security solutions that protect information in motion, such as that exchanged within and between organizations, as well as information services or applications that can be readily accessed via the Internet, such as web servers. These security functions must also include mechanisms for establishing trust and verifying identity across networks. More specifically, security architectures must be developed that provide the following guarantees [Bhi98]:

- Confidentiality: the guarantee that the contents of a message are private and protected from disclosure;
- Authenticity: the guarantee that a message comes from the individual who appears to have sent it or the guarantee that an individual is authorized to access a service or system based on an electronic identity;
- Integrity: the guarantee that the message contents have not been modified or duplicated, either purposefully or incidentally;
- Nonrepudiation: the inability of an individual to renege on a transaction or deny participation in communication after the fact;

- Availability: the assurance that authorized users will have reliable and timely access to required information resources and communication services [DON99].

Figure 1-1 illustrates the Department of the Navy's (DON) Defense in Depth approach for achieving a layered, redundant, and comprehensive network security architecture. Each layer of the model incorporates a collection of devices, applications, and procedures for implementing a structured, complimentary defense against a variety of potential attacks. A PKI is a critical component of this architecture that supports confidentiality, authentication, integrity, and nonrepudiation by providing for the secure generation and distribution of digital certificates and cryptographic keys. A PKI operates across all four zones of the DON defense-in-depth model, interacting with and providing services to other security systems and components. For example, a virtual private network (VPN) device can use the attributes of digital certificates to specify encryption algorithms and key lifetimes, while a firewall can use digital certificates for authentication and access control [Fra99]. A PKI is not an independent, silver bullet solution for all network security threats. Instead, it is central component of an overall security architecture and strategy that operates in unison with other security systems to provide in-depth, robust, and mutually supported defense against a myriad of potential network threats.

This thesis addresses the management and technological challenges faced by the Marine Corps in developing and implementing a Marine Corps PKI within the framework of the DoD PKI. How should the Marine Corps proceed to meeting DoD's requirements,

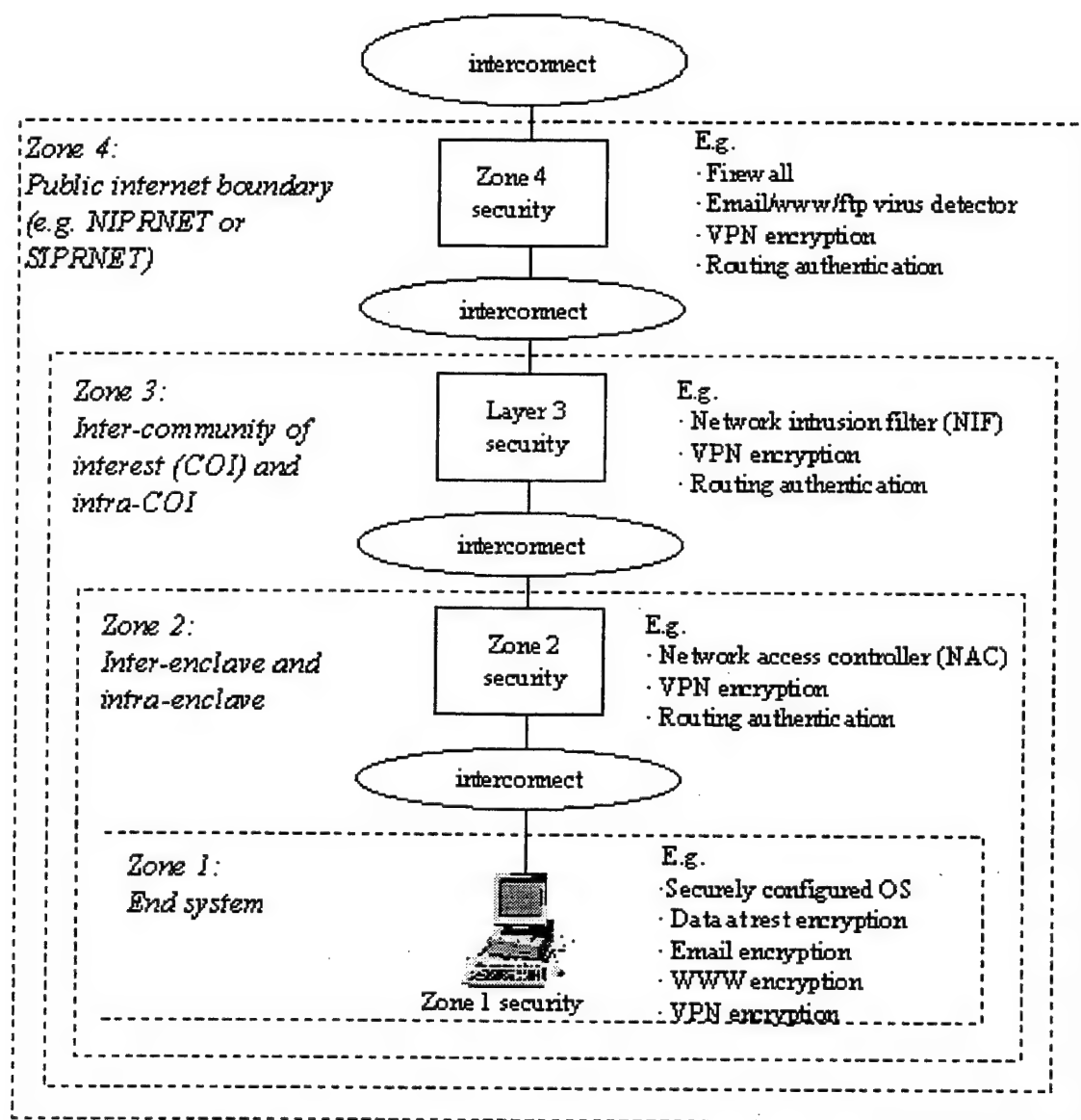


Figure 1-1. Defense in Depth Concept [DON99]

while simultaneously avoiding the pitfalls of developing a PKI before the technology fully matures and stabilizes? How can the Marine Corps address its own unique requirements and design its PKI services to meet these, while still remaining fully integrated with the DoD PKI? What strategy should the Marine Corps adopt to meet an

aggressive DoD timeline and still remain within budgetary constraints? Finally, how can the Marine Corps manage the change introduced by the incorporation of public key cryptography into daily operations? The focus of this thesis is to describe these problems in greater detail, outline Marine Corps' objectives for developing a PKI, and recommend solutions and strategies based on the objectives.

The thesis begins by describing the elements and capabilities of a PKI. The DoD PKI model is summarized and defined in the context of the DoD's overall Defense in Depth concepts. Next, Marine Corps' roles, responsibilities, and strategies for developing a PKI are outlined and defined. Technical and managerial challenges are then identified and explained. Finally, the impact and management of change resulting from the implementation of a PKI across the DoD and within the Marine Corps is examined and discussed.

Chapter II introduces public key cryptography as an emerging technology that provides mechanisms supporting each of these guarantees defined above. Public key cryptography differs from conventional cryptography in that two mathematically related, yet different keys are used for encryption and decryption, instead of identical copies of the same key. Where conventional cryptography is limited to providing confidentiality and integrity, public key pairs can be used to provide confidentiality and integrity, as well as authentication and nonrepudiation. However, before public key systems can be widely and effectively deployed, a number of issues must be addressed to ensure that the technology is used correctly and confidently.

Foremost among these issues is the presence of a PKI to provide essential services, such as identity verification, user registration, and key distribution. More importantly, a PKI is deployed to establish a network of trust, enabling a public key system to provide true authentication and nonrepudiation services. This network of trust is critical for equipping users and applications with the confidence necessary to utilize public key mechanisms. Without the basis for trust, a sufficient level of user confidence is not achieved and a public key system does not adequately address the guarantees described above. In the second half of Chapter II, the need for a PKI is explained, the elements of a PKI are discussed, and the functionality of the PKI elements for establishing and maintaining system trust are described.

Chapter III begins with a description of the Department of Defense's (DoD) PKI development efforts. The DoD PKI is discussed in the context of the DoD's overall information assurance (IA) efforts and is described as the central element in the defense in depth strategy embraced by the DoD for providing a structured, layered, and redundant security across all DoD networks. The DoD's PKI general structure and supported levels of information assurance are also discussed. This leads into the primary focus of Chapter III – defining the Marine Corps' roles and responsibilities within the overall DoD PKI. Marine Corps specific PKI architectural elements are identified and objectives are outlined for meeting DoD mandates and timelines. Strategies for meeting the objectives are proposed and potential risks and challenges are highlighted. Finally, a Marine Corps PKI development process is presented as a model for pursuing Marine Corps' objectives and strategies.

In Chapter IV, major technology challenges in the development and implementation of a Marine Corps PKI are identified and described. The requirement for system scalability to support a growing number of users and applications is explained and the critical need to provide for and support interoperability, both internal and external to the DoD, is emphasized. PKI Directory Services are identified as one of the most challenging components of PKI development efforts. Specific PKI directory challenges discussed in Chapter IV include directory scalability to accommodate a rapidly growing user base. Obstacles and recommended solutions for achieving directory interoperability with other directory applications within the Marine Corps and DoD, as well as with external PKIs, are also discussed. Additional topics include the support for key escrow and recovery mechanisms; certificate verification techniques and procedures; and private key storage technologies.

Chapter V focuses on how the Marine Corps should manage change leading up to the widespread deployment of a PKI. Although the Marine Corps as a military organization will in no way be transformed by the implementation and utilization of public key systems, the way Marines conduct daily operations over computer networks will be significantly altered. Not only will computer users need to be familiar with the basic concepts of public key cryptography, they must be better informed about the types of network threats and the procedures, services, or systems that protect against these threats. A full implementation of a PKI within the Marine Corps will affect every Marine and civilian employee, as well as contractors, suppliers, and most other entities that interact with the Marine Corps across computer networks. Chapter V addresses the issues

resulting from this change and provides strategies for facilitating and mitigating the negative impact of change. Topics include establishing a vision for change; the development of strategies for change; strategic choices for enabling change; and overcoming resistance to change.

Chapter VI summarizes the key points of the thesis and presents general conclusions based on the overall research for the thesis. The implementation of a PKI within the DoD and Marine Corps is a complicated and diverse process that requires careful and methodical planning to ensure that it is operationally effective and properly integrated into the existing network and security architectures. Although this thesis presents a broad overview of many of the most important and pressing issues, other relevant issues for implementing a PKI must be considered. Chapter VI identifies and briefly discusses additional issues for further research.





## II. PUBLIC KEY CRYPTOGRAPHY AND INFRASTRUCTURES

Public key cryptography was developed by Whitfield Diffie and Martin Hellman in May 1975 to solve two inherent problems of conventional, secret-key cryptographic systems: digital authentication and secure key distribution [Dif98]. Conventional, or symmetric, cryptography employs the same key for both encryption and decryption, requiring all communicating parties to have a copy of the same key. However, simple possession of a symmetric key does not guarantee that a party is both authorized to read the message and is authenticated as the intended recipient [Gra97]. Since all communicating parties must have an *identical* copy of the same key, symmetric keys do not have a mechanism for differentiating, and therefore authenticating, among individuals within an organization or between individuals across networks. Confidence of identification over networks is not as simple as looking at a picture ID. Although the originator of a message encrypted with a symmetric key may claim to be a certain individual, no mechanism is provided to authenticate the originator's identity and, therefore, the originator could actually be *anyone* with access to the symmetric key.

Key distribution is the second problem of symmetric cryptography studied by Diffie and Hellman. Ensuring that all parties requiring communication have a copy of the secret key is no easy task, particularly when there is a large community of users who may or may not know each other. If a key expires or is compromised, then new keys must be distributed to all parties. Stringent management procedures must be established to track the distribution of keys, ensuring that the keys are only distributed to authorized parties and that all parties are using the same, current version of the secret key.

Diffie and Hellman recognized that the problems of key distribution and digital authentication imposed significant limitations on the scalability and validity of conventional symmetric cryptographic systems utilized across intranets and internets. From their research, the concept of inverse key pairs emerged in which each key pair has two properties:

- Information encrypted with one key can ONLY be decrypted with the other key of the pair.
- Given one member of the key pair, the *public key*, it is infeasible to discover the other, the *private key*.

The inverse property of the two keys and the resulting separation of encryption and decryption encompass the foundation for public key systems by providing a single solution to the problems of key distribution and digital authentication. Public key cryptography, also referred to as "asymmetric cryptography," offers several advantages over symmetric cryptography, including the facilitation of key distribution and the ability to digitally sign messages for proof of identity [DOD97].

#### **A. SYMMETRIC CRYPTOGRAPHY**

To better understand the advantages of public key cryptography, a further description of symmetric cryptography is required. Suppose that two parties, Bob and Alice are working together on a project that requires frequent exchanges of sensitive information. Bob and Alice are geographically separate and decide that the best way to exchange information is over the Internet. However, due to the sensitive nature of the

information, it must be protected from eavesdropping, therefore Bob and Alice decide to encrypt the information prior to transmission.

Figure 2-1 demonstrates symmetric cryptography: the exchange of information using a common, secret key. Alice encrypts a message with her copy of the key and transmits the encrypted message to Bob. Bob is able to decrypt the message since he possesses an identical copy of the key Alice used to encrypt the message [DOD97]. Eavesdroppers may intercept the encrypted message, but they will not be able to decrypt it without knowledge of the secret key [Feg98]. This transaction requires prior communication between Alice and Bob by secure means so that they may agree upon a key for the session.

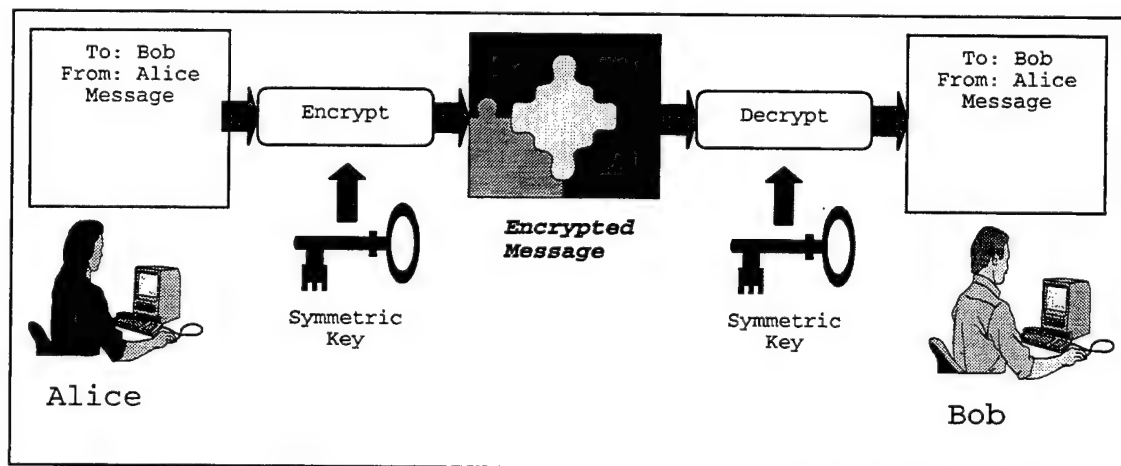


Figure 2-1. Symmetric Key Encryption

The encryption of plaintext and decryption of unintelligible ciphertext by symmetric keys is accomplished utilizing secret-key cryptographic algorithms. Cryptographic algorithms are mathematical functions that specify the encryption or

decryption steps executed when applying the cryptographic keys. Using the shared secret key, secret-key algorithms to encrypt plaintext messages to ciphertext messages that are usually about the same size [Feg98]. Although several secret-key algorithms exist, the official U.S. government standard is the Data Encryption Standard (DES) [DON99]. DES employs a key size of 56 bits and is the most widely used cryptographic algorithm in the world. Although this is more than sufficient for many applications, highly sensitive information may call for more stringent protection. Using multiple encryptions can increase the effectiveness of DES. Triple DES involves the initial encryption with key 1, followed by a decryption of the result using key 2, followed by an encryption of that result using key 3 [For98]. Keys 1 and 3 may be same or different, resulting in the application of two or three 56-bit keys. This variant on the DES algorithm is several orders of magnitude stronger than standard DES and may be used by DoD organizations in lieu of DES [DON99].

A major challenge of symmetric cryptography is secure key distribution. Although this may be relatively uncomplicated for small organizations, the problem becomes increasingly challenging for large, geographically dispersed organizations. Larger organizations may establish centralized key distribution centers (KDC) to address the problem of symmetric key distribution and exchange. A KDC is a trusted third party that shares a secret key with each subscriber and uses these keys to provide additional keys to the subscribers as needed [Dif98]. Subscribers needing to communicate securely must first contact the KDC to obtain a secret session key for use during their communication. However, KDC's do not scale well and require considerable

administrative efforts to efficiently manage operations [Feg98]. Public key cryptography significantly simplifies the problem of key exchange, thereby creating many new possibilities for the use of cryptography in current and emerging applications.

## **B. CONFIDENTIALITY**

Public key cryptography utilizes key pairs of which only one, the private key, must be kept secret. The public key may be distributed freely or published in a directory [DOD97]. This is possible due to the inverse property of the two keys: a message encrypted with a public key cannot be decrypted with that same key. Only the public key's secretly stored partner, the private key, can decrypt the message. The keys cannot be derived from each other, so the wide availability of the public key does not compromise the private key.

The inverse property of the keys in a pair is a function of the mathematical relationship derived from a public-key algorithm. Each key contains the necessary mathematical information to decrypt messages encrypted with the other. The most popular public-key algorithm, RSA (named after its creators, Rivest, Shamir, and Adleman), uses a variable key length between 512 to 2048 bits and is based on integer factorization. RSA depends on the fact that multiplying large prime numbers is computationally easy, but that factoring a large number into its prime factors is computationally very difficult. Therefore, the knowledge of the prime factors can be kept secret and used to derive the private key, while the number resulting from multiplying the prime factors can be made public and used as a basis for the public key [Feg98].

Figure 2-2 demonstrates the encryption mechanism used for message confidentiality. Confidentiality, or secrecy, ensures that information is not disclosed to unauthorized parties [Feg98]. Alice uses Bob's public key to encrypt a message and transmits it to Bob, who uses his protected private key to decrypt it. Confidentiality of the message during transmission is ensured since only Bob's private key can decrypt a message encrypted with his public key [DOD97]. In application, the algorithms used for public key cryptography are about 100 to 1000 times slower than secret key cryptography [Feg98]. Consequently, a better method involves the use of a hybrid system in which public key mechanisms are initially used for the secure establishment of shared keys for

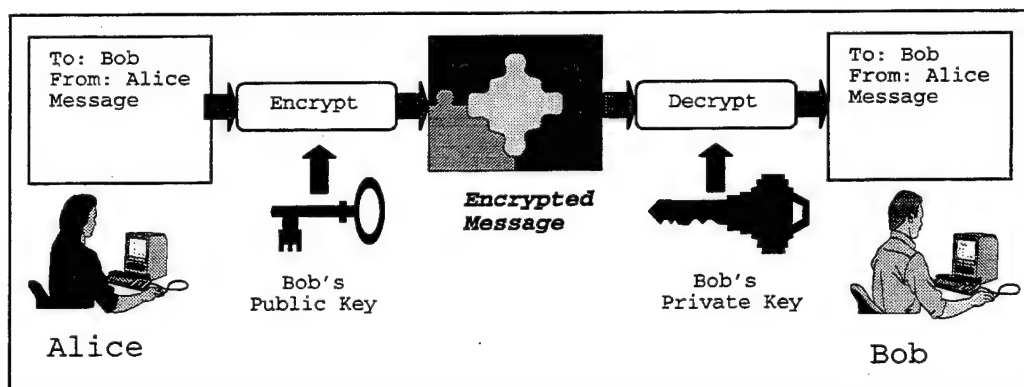


Figure 2-2. Public Key Encryption for Confidentiality

use with conventional, symmetric cryptography [Dif98]. A hybrid system can be used in many different variations. In a simple example, Alice uses a symmetric key to bulk encrypt information to be sent to Bob. She next uses Bob's public key to encrypt the symmetric key used for the encryption. The encrypted information and encrypted symmetric key are sent to Bob, who uses his private key to decrypt the symmetric key.

The decrypted symmetric key is now used to decrypt the information from Alice [DOD97].

### **C. AUTHENTICATION AND INTEGRITY**

Authentication in the form of digital signatures is another advantage of public key cryptography. Authentication refers to the process used to ascertain the identity of a person or the integrity of specific information [DOD99]. Integrity refers to the consistency of data; in particular, preventing unauthorized creation, alteration, or destruction of data [Bau97]. Once again, the inverse property of the key pairs provide for the authentication and integrity mechanisms. A message encrypted with an individual's private key can only be decrypted and read with that individual's public key. Since private keys are kept secret, a message decrypted with an individual's public key must have been encrypted by that same individual using the private key. Therefore, encrypting a message with a private key creates a type of "digital signature" over the message. This process outlines the basic concept of digitally signing a document with a private key, but does not represent the more common, standard description of digital signatures. A more accurate description of digital signatures is given later in this section. Decryption of a digital signature with a public key to verify the sender's identity is called signature verification [Feg98].

Although authentication by decrypting with the public key confirms that the holder of the private key sent the message, it does not guarantee that the person possessing the private key is who they say they are. What has really been authenticated is



that the sender has a copy of the private key used in the transmission. There is no assurance that an imposter has not obtained a copy of someone else's private key and is

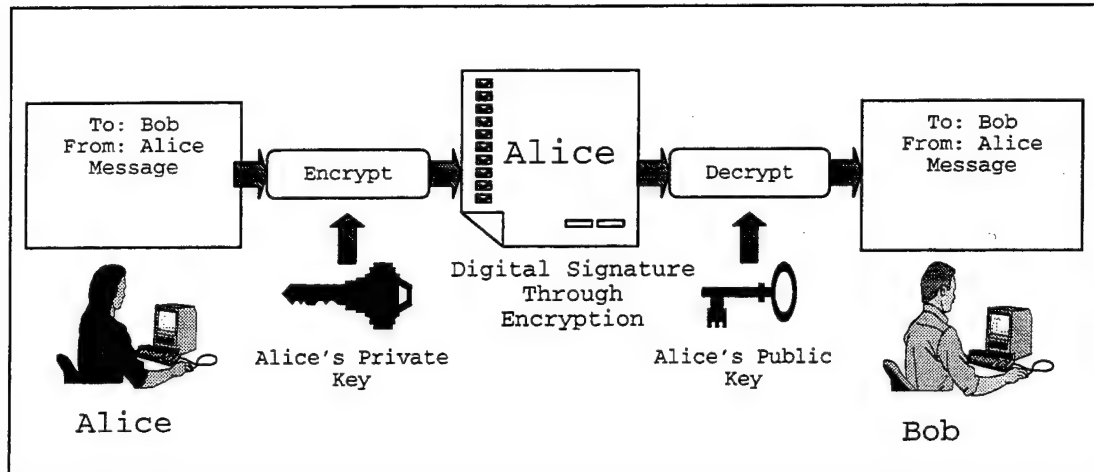


Figure 2-3. Basic Authentication with Public Key Pairs

using it to impersonate that individual by digitally signing messages. If two communicating parties have never actually met, it may be difficult for the receiver to discover that a message is not from the expected party. Certification authorities (discussed later in this chapter) address this problem by acting as a trusted third party that certifies the identities of communication parties.

Due to the processing expense of both the signature process (encrypting the message with the secret key) and the verification process (decrypting the message with the public key), the actual authentication and integrity process encrypts a digest of the original message rather than the entire message [Dif98]. Therefore, the more standard application of digital signatures results from encrypting a message digest with a private key rather than the entire message. A message digest, or hash, is created by using a one-

way function known as message-digest algorithm, which takes a variable-length message as input and produces a fixed-length message as output [Feg98]. The resulting hash is like a fingerprint of the message: it is computationally infeasible to find another message that would produce an identical hash [DOD97]. For instance, if the fixed-length output of a message digest has  $m$  bits, it would take approximately  $2^m$  messages to find a message with a desired digest, and  $2^{m/2}$  messages to find two messages that have the same digest [Feg98]. Therefore, if a digest length is 160 bits,  $2^{80}$  messages would need to be searched to find an identical hash. The hash can also be used to verify the integrity of the message since a modification to the original message during transit will result in a different hash. Two of the most widely used message digest algorithms are the Secure Hash Algorithm-1 (SHA-1) and the Message Digest-5 (MD-5) [DON99].

The generation and verification of a digital signature using a digest are illustrated in Figure 2-4 [Feg98]. Alice uses a message-digest algorithm to calculate the hash of a message to be sent to Bob and encrypts (signs) the hash using her private key. The message and the signed hash (digital signature) are transmitted to Bob. By using Alice's public key to decrypt the digital signature created by Alice's private key, Bob verifies that the message was encrypted with Alice's private key, thus "authenticating" the origin of the message. Additionally, Bob uses the same message-digest algorithm to compute a local copy of the hash from the message. By comparing the expected hash received from Alice to the actual hash computed locally, Bob can verify the integrity of the message, provided that the values are identical. Any differences between the two hashes indicate that the message was changed or modified in transit. For this application, Alice's private

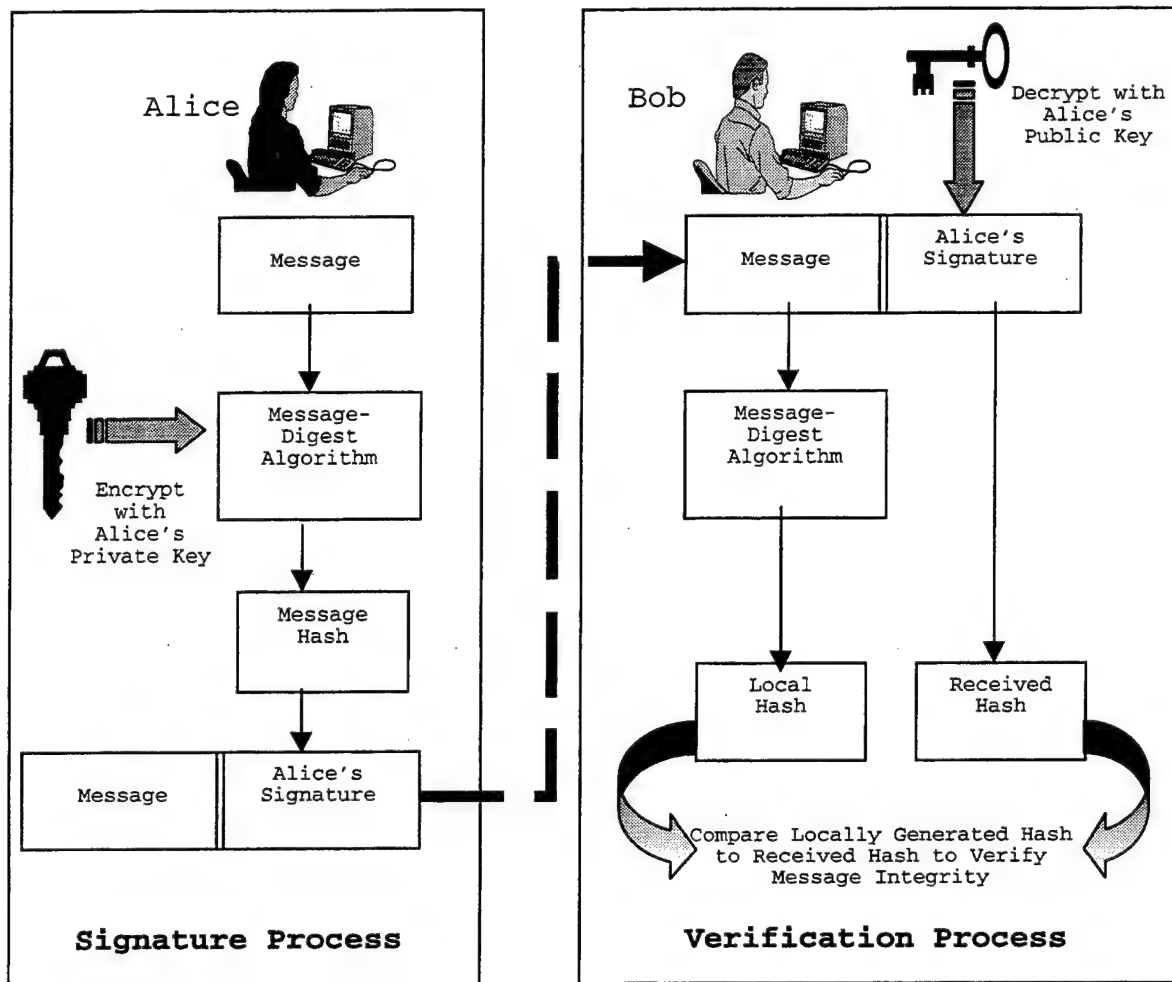


Figure 2-4. Digital Signature Generation and Verification

key is referred to as a signing key and her public key is referred to as a verification key [Feg98].

#### D. ESTABLISHING TRUST

Correctly used, digital signatures should provide the following assurances [Gra98]

(See Chapter 1 definitions of security guarantees):

- Authentication: Assurance of identity; verification that an individual or entity is who they claim to be.
- Message integrity: Confidence that the message arrived unmodified, unduplicated, and properly created.
- Nonrepudiation: Confidence that a party involved in a communication cannot deny participation in the communication. Because key pairs are unique, the sender cannot deny having sent the message.

In the example from the last section, Bob uses Alice's public key to decrypt her digital signature and verify that the message came from Alice. However, how does Bob know that "Alice" is who she claims to be? Through the authentication process, Bob has actually only determined that the message was sent by the owner of the private key that created the digital signature. To establish trust, a mechanism must exist to bind a particular individual or organization to a specific private key, thereby ensuring that the private key used to sign the digest truly belongs to the sender [Gra98]. Without a binding of a signature to an identity, the digital signature is useless.

A digital certificate is a binding between an individual's or entity's identity and a public key [Feg98]. The digital certificate "certifies" that the identified individual or entity is the owner of the private key associated with the corresponding public key contained within the certificate. For the binding to be valid, it must be performed by a trusted third party known as a Certification Authority (CA). The primary function of a

CA is to confirm the identity of subscribers and issue digital certificates associated with the public key pair of the subscriber [Feg98].

The issuance of certificates is analogous to the issuance of military identification (ID) cards. Only designated administrative activities may issue ID cards and they are only issued to authorized individuals based on their military status, affiliation, or association. Most importantly, designated activities must ensure the identity of the recipient through proper credentials before issuing an ID card. Special equipment is used to produce ID cards and complicated holograms are included on the cards to help prevent forgery. Similarly, CAs must have established procedures for verifying the identity of subscribers and, if necessary, confirming their affiliation to an organization.

Additionally, CAs must ensure that the certificates they issue cannot be forged. After verifying the identity of a subscriber, CAs digitally sign certificates with their own private key, thereby incorporating their own digital signatures into the certificate [Feg98].

Similar to the signing description in the last section, a CA computes a hash of the certificate and encrypts it with its private key. The signature authenticates that the certificate was issued by that particular CA and ensures the integrity of the certificate.

## **E. PUBLIC KEY INFRASTRUCTURES**

The establishment of a CA is the first step in the establishment of an infrastructure to support public key mechanisms and the issuance of digital certificates. The requirements and the size of an organization will determine the scope and consistency of the infrastructure required to support its operations. A public key infrastructure (PKI) is that portion of the security management infrastructure dedicated to the management of

keys and certificates used by public key-based security services [DOD97]. Correctly managed, digital certificates provide an efficient system for communication authentication as well as a secure, scaleable method to distribute public keys in large communities [Feg98]. Public keys are electronically stored with their associated certificates so that they are publicly accessible and easily downloaded. A PKI provides the necessary support structure to establish a trusted public key framework, thereby ensuring the validity of digital signatures, and making the use of public key mechanisms feasible within and between numerous applications.

A PKI consists of multiple components working together to ensure users, entities, and applications can utilize public key mechanisms for authentication, integrity, non-repudiation, confidentiality, and authorization services. Three primary elements must be in place to achieve these services: certificate management, registration, and public key enabled applications [DOD99]. Each element has distinct responsibilities that must be met to achieve a fully functional, robust, and secure infrastructure capable of establishing and maintaining a chain of trust throughout the PKI. The components and responsibilities of the three elements of a PKI will be discussed in the following sections.

## **1. PKI Elements**

The three primary elements of a PKI are discussed in the following sections.

### ***a) Certificate Management***

Certificate Management (CM) is comprised of components that provide for the generation, production, distribution, control, accounting, and destruction of public keys and digital certificates [DOD99]. The components responsible for these functions

are the Certification Authority and Directory Services. As mentioned previously, the establishment of trust with the CA serving as a trusted third party within a PKI is essential to the successful operation of a PKI. Therefore, the most critical function of CM is to certify the identity of individuals or entities possessing public keys pairs and the associated digital certificates.

The CA, which is the central component of a PKI, performs the following functions [DOD99]:

- Establishing and providing policies, procedures, and guidance for the operation and management of the PKI. Training, support documentation, and user tools must be provided to the personnel responsible for user registration.
- Registration of subordinate CAs and Registration Authorities (RA).
- Generating, signing, and issuing certificates to users and entities. Each certificate is signed by the CA's private key, thereby certifying the identity of the possessor of the corresponding private key.
- Managing the revocation of certificates by maintaining a certificate revocation list (CRL) and/or providing for real time verification of certificate status.
- Archiving all certificates (including the associated public key) and CRLs, beyond expiration or revocation, to support non-repudiation services.
- Establishing mechanisms and procedures for key escrow and key recovery to support the recovery of private keys used for purposes other than non-repudiation.

When using public key cryptography to encrypt a message or to verify another user's digital signature, a user must first obtain a copy of the necessary public key stored with the other user's digital certificate. Directory services, the other component of CM, provide a repository from which users and applications may obtain the digital certificates of other users and revocation information such as CRLs [DOD98a]. Additionally, white pages information may be maintained in directories that include information such as user email addresses, phone numbers, and other personal or organizational information. Although many of the directory services functions are maintained at the CA, the overall directory structure is often distributed and replicated throughout an organizational PKI, particularly as the size of the PKI increases.

Certificates are used as the mechanisms for establishing trust within and between PKIs [DOD99]. Within a single PKI, trust (confidence of identity) is validated by the CA's digital signature on the certificates it issues. The CA's digital certificate is publicly available to users and applications to verify the validity of the CA's signature by decrypting it with the CA's public key. Between PKIs, relationships of trust may be established that allow users and applications to "trust" certificates issued by other PKIs. These relationships are usually established through formal agreements between the respective CAs. Provided that the PKIs are interoperable, users in one PKI wishing to exchange information with users in an external trusted PKI may download public certificates from the external PKI's directories. As certificates are a means of conveying



trust, directory services are the instruments for distributing that trust, as well as other information, throughout and between PKIs.

***b) Registration***

Before a CA can issue a certificate to a user, the user must register with the CA by submitting a certificate application. Registration involves the establishment of a relationship between an applicant and a CA, and the recording of certain applicant information with the CA [Bau97]. For small, localized PKIs, the entire registration process may be done directly between an applicant and a CA. However, larger, geographically dispersed PKIs usually rely on Local Registration Authorities (LRA) to act as intermediaries between applicants and a CA to ensure that users are who they claim to be, i.e. authorized to obtain certificates from the CA. LRAs operate the software necessary to interface with the CA. Large PKIs with many LRAs may develop a hierarchy with a smaller number of Registration Authorities (RA) established to register LRAs [DOD97]. Primary responsibilities of an RA may include:

- Approving, creating, and terminating LRAs. RAs may issue LRA certificates (signed by the RA) after ensuring the identity of the LRA.
- Revoking certificates, as required.
- Updating CRLs and white page information pertaining to users registered via the RA or its LRAs.
- Providing the appropriate policy, guidance, and training to registered LRAs.

RAs should register a sufficient number of LRAs so that each LRA is geographically located with its users and is able to effectively manage new applications and certificate renewal requests. In most instances, identity verification of users must be done face to face with an LRA. Therefore, users should not have to travel an unreasonable distance to register with an LRA. It is the responsibility of the RA to establish an appropriate number of LRAs within the RA's area of responsibility and to ensure that the LRAs are properly dispersed to meet the needs of all authorized users. Additionally, users registering with an LRA are immediately registered with the CA and, subsequently, cannot attempt to register again with another LRA, since their unique registration information is already recorded within the PKI.

*c) Public Key Enabled Applications*

A PKI's role will be very limited without the presence of applications that can utilize its services. In the age of the information revolution, organizations often acquire new, state-of-the-art equipment and information technologies before fully understanding the capabilities of the technology or the impact of implementing the technology within an organization. In a PKI-enabled organization, application developers or purchasers must understand the PKI's policies, usage, and interfaces [DOD99]. Applications must be developed or acquired that are not only PKI-enabled, but also fully interoperable and functional with the existing infrastructure. Without full interoperability, separate, technologically isolated PKIs may emerge within an organization to support specific applications. This will lead to user confusion as users

will be required to possess certificates for each such application and will need to be familiar with the policies of each PKI.

## **2. PKI Hierarchy**

A single PKI can be viewed as a hierarchical structure with the CA at the top, RAs in the middle, and LRAs at the bottom. However, many PKIs are part of larger infrastructures with multiple CAs subordinate to a root CA. The root CA is at the very top of the hierarchy and is responsible for issuing certificates to subordinate CAs, thereby verifying their identities and authorizing them to issue their own certificates. In some models, Subordinate CAs may sign certificates for other CAs, creating their own Subordinate CAs. Subordinate CAs are often referred to as Signing CAs since they are responsible for "signing" user certificates. For this text, however, a "Signing CA" will be referred to simply as a "CA." The policies of CAs must be developed in accordance with those of the root CA, requiring approval by the root CA [Cho94]. A simplified hierarchical structure of a PKI from the root CA down is illustrated in Figure 2-5. Although several variations of this hierarchy exist, each with varying levels of complexity, this model closely resembles the DoD PKI and will be the model of reference for this text.

## **3. Certificate Generation and Distribution**

During registration, subscribers submit an application containing specific information to be used in the generation of their digital certificates. However, digital certificates are more than a collection of data elements signed by a CA's private key. A

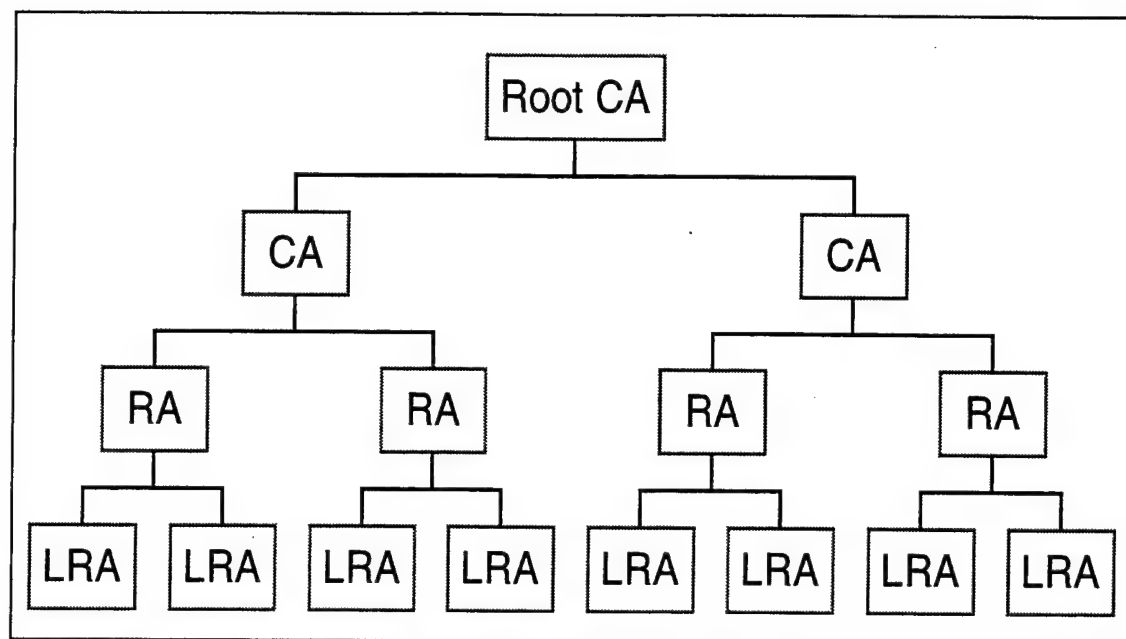


Figure 2-5. PKI Hierarchical Structure

certificate needs to be an extensible data structure, customizable to meet the requirements of various certificate-using environments [Feg98]. For example, a certificate used strictly for identification purposes may contain very generic and basic attributes such as name and social security number; however, a certificate used for email confidentiality should include additional attributes such as email address and organization.

A critical component of any certificate-using environment is the directory service. To meet the requirements of online directory services such as those needed for a PKI, the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) published a directory standard known as X.500. The X.500 standards provide the basis for constructing a multi-purpose distributed directory service by interconnection computer systems belonging to service providers, governments, and private organizations, potentially on a global scale [Bau97].

Recognizing the potential for using X.500 directories for distributing public key certificates, ITU and ISO included the specifications for the data items required to fill this role and designated the standard certificate format X.509. The X.509 standard was first published in 1988 as part of the X.500 Directory recommendations and is currently in its third version, designated X.509 v3 [Feg98]. With a standard certificate format, software developers can theoretically write generic code that works with all X.509 certificates and users will not need to obtain separate certificates for each specific application. X.509 v3 includes definitions for standard extension fields, such as those for conveying additional subject identification information, key attribute information, and policy information [Feg98].

In addition to certain personal information, a user's public key must be included in a digital certificate before being issued to applicant and published in a directory. Key pairs are usually generated one of two ways: at the user's local system or at a central system [Feg98]. For key pairs generated local to the user, the public key must be transferred to the CA along with the certificate application and the private key must be securely stored on the local machine or on a form of removable storage such as diskettes or smart cards. Smart cards, which are read by smart card readers, are credit-card sized tokens that contain a microprocessor and memory to store programs and data [Feg98]. In some applications, key pairs may be generated and stored on smart cards. Regardless of the storage method, the private key is generally encrypted and protected with a PIN.

Key pairs may also be generated at a central system, such as the CA itself or an associated system. The central system must then forward a copy of the public key to the

applicant (and the CA if the central system is not part of the CA) and securely transfer the private key to the applicant [Feg98]. This approach may have advantages over generating key pairs locally in that the central system may have the resources and controls to generate higher quality keys and, if required, can locally back-up or escrow private keys for key recovery purposes before transferring them to end-users [Bau97]. However, keys used for nonrepudiation services cannot be backed-up or escrowed since only the owner of the private key may possess a copy for true nonrepudiation services. Key escrow and recovery will be further discussed in Chapter IV.

Once the CA has processed a user's application and has received a copy of the public key, the X.509 certificate is generated and signed with the CA's private key. The completed digital certificate is then forwarded to the user and copied to the PKI's X.500-based directory service. Anyone then needing to securely transfer information to the new certificate holder may obtain a copy of his or her public key by downloading a copy of the associated certificate from the directory service and encrypting the information with the user's public key. Additionally, users who receive a signed message from the new certificate holder can authenticate the user and verify the validity of the signature by decrypting it with the user's public key. The certificates received from the Directory Services may also be verified by decrypting the digital signature on the certificate with the CA's public key.

Users and applications often include a copy of their public key and certificate with their transactions. This alleviates the requirement to download the certificate from the CA's directory. However, the certificate may still need to be checked to ensure that it is

still valid and has not been revoked. This may be accomplished by checking a certificate revocation list (CRL) or by accessing an online status-checking repository. A CRL is a time-stamped list of revoked certificates, identified by certificate serial number, that has been digitally signed by the responsible CA and posted to the CA's X.500 directory service or to a known Web page [Bau97]. Users and applications check the CRL to ensure that a particular certificate has not been revoked. An important limitation of CRLs is that the list will not reflect any certificates revoked since the last issuance of the CRL. Depending on the value and sensitivity of information exchanged, this may be a critical consideration when attempting to verify the status of a certificate. The interval between publishing of CRLs is a policy decision for a particular CA, therefore, it may vary significantly between different CAs. Another disadvantage of CRLs is that they are often distributed to local directories, which may be cumbersome to networks depending on the size of CRLs and frequency of new publications.

As a dynamic option to CRLs, a certificate-using application may execute an on-line query with a CA to determine the revocation status of a certificate [Feg98]. This method avoids the time granularity by returning the currently revocation status of the certificate in question. The requirement to distribute large CRLs to local directory systems may also be eliminated. However, online status checking does not come without a cost. CAs using this method must operate and maintain a trusted data repository server that is available at all times [Feg98]. Also, since the repository server must digitally sign each query to ensure its validity, the processing expense for this method may be great, potentially creating a bottleneck at the server. Networks must also possess the necessary

bandwidth to deal with the added traffic resulting from the on-line queries. On-line status checking across bandwidth-constrained networks result in unacceptable overall network performance.

## **F. CONCLUSION**

This chapter introduced public key cryptography and compared it to conventional symmetric cryptography. The advantages of public key cryptographic systems were discussed in terms of key distribution and digital authentication. The utilization of public key cryptography to achieve confidentiality, authentication, integrity, and nonrepudiation was demonstrated and the need to establish a framework of trust for public key-enabled systems was identified. Digital certificates were defined as the mechanisms for conveying trust. Public Key Infrastructures were shown to be essential for providing the structure, policies, and procedures for issuing, distributing, and verifying digital certificates. Chapter III outlines Marine Corps' roles and responsibilities within the DoD PKI and discusses specific objectives and strategies the Marine Corps should pursue in the development of its own PKI elements.





### **III. USMC PKI ROLES, RESPONSIBILITIES AND OBJECTIVES**

#### **A. INTRODUCTION**

In Chapter II, public key cryptography was introduced and the primary elements and general organization of a PKI were discussed. The Department of Defense (DoD) Public Key Infrastructure (PKI) Roadmap establishes the enterprise-wide end-state for a DoD PKI and outlines the DoD strategy and timeline for the availability of PKI capabilities [DOD99]. Roles and responsibilities for implementing PKI within DoD are assigned and critical issues are identified. The purpose of this chapter is to make recommendations for the framework within which the Marine Corps will develop its own elements of the overall DoD PKI and to set Marine Corps-specific targets within the scope of the DoD PKI Roadmap.

The DoD's and Marine Corps' PKI implementation will be an integral part of the Information Assurance (IA) efforts of the Marine Forces Computer Network Defense (MARFOR-CND), which is the Marine Corps' subset of the Joint Task Force Computer Network Defense (JTF-CND) initiative. Since the DoD PKI is still in the early stages of development and implementation, the objectives outlined in this preliminary USMC Roadmap are not definitive and may change as the DoD PKI evolves and PKI technologies mature. Instead, a foundation is built from which USMC PKI efforts may further plan, refine, and develop the final architecture and policies.

## **B. INFORMATION ASSURANCE AND THE DOD PKI**

### **1. Achieving Information Assurance**

Information Assurance (IA) refers to information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation [DOD98a]. The Deputy Secretary of Defense Memorandum, subject: Department of Defense Public Key Infrastructure states:

Achieving Information Superiority in a highly interconnected, shared-risk environment requires that DoD's Information Assurance (IA) capabilities address the pervasiveness of information as a vital aspect of warfighting and business operations. To do so, DoD must provide integrated voice, video, and data transmission services that meet both warfighting and business needs as an integral part of DoD's global information enterprise. The technical strategy that underlies DoD IA is Defense-in-Depth, in which layers of defense are used to achieve our security objectives... One element of the Defense-in-Depth strategy is the use of a common, integrated DoD PKI to enable security services at multiple levels of assurance [DSD99].

The foundation for the Defense Information Infrastructure's (DII) IA capabilities is the DoD Key Management Infrastructure (KMI), of which the DoD PKI is an essential element and major component [DOD98a]. DoD's Electronic Key Management System (EKMS) will be integrated with the DoD PKI and any other pertinent key management initiatives to form the DoD KMI. EKMS currently provides symmetric cryptographic key management and distribution services [DOD99a]. The Defense-wide Information Assurance Program (DIAP) provides oversight of DoD PKI planning and execution activities to ensure consistency with DoD's overall IA objectives, and the various initiatives that will implement those objectives [DOD99a]. To achieve the DoD's goal of

Information Superiority, the Marine Corps must develop a PKI as one of several strategies, architectures, and mechanisms necessary to provide a layered structure of IA capabilities.

## **2. DoD PKI Structure**

In accordance with the DoD PKI Roadmap, Chapter II describes three elements of a PKI: certificate management, registration, and PKI-enabled applications. This section describes the structure of the DoD PKI and the roles and responsibilities of the agencies supporting the PKI. The elements discussed in Chapter II can be further delineated into specific components encompassing four organizational levels (See Figure 3-1). The DoD Root CA, owned and operated by the National Security Agency (NSA), represents the top level of the DoD PKI. The Root CA's certificate is used to establish all subordinate CAs within the DoD and is, therefore, the DoD PKI's authoritative source of authenticity for all certificates created within its domain [DOD97]. Since a compromise of the Root CA will result in the total compromise of the DoD PKI, it is operated off-line and is protected by stringent physical security.

The second level of the DoD PKI consists of the CAs and the associated Directory Services. CAs consist of the personnel and equipment (CA servers) authorized and trusted by the Root CA to issue certificates to end-users and provide information to the DoD PKI Directory Services [DOD99a]. The DoD PKI Roadmap projects that the CAs that support classified, mission, critical, command and control applications will be owned and operated by the DoD, under the direct control of the DoD Root CA. The final

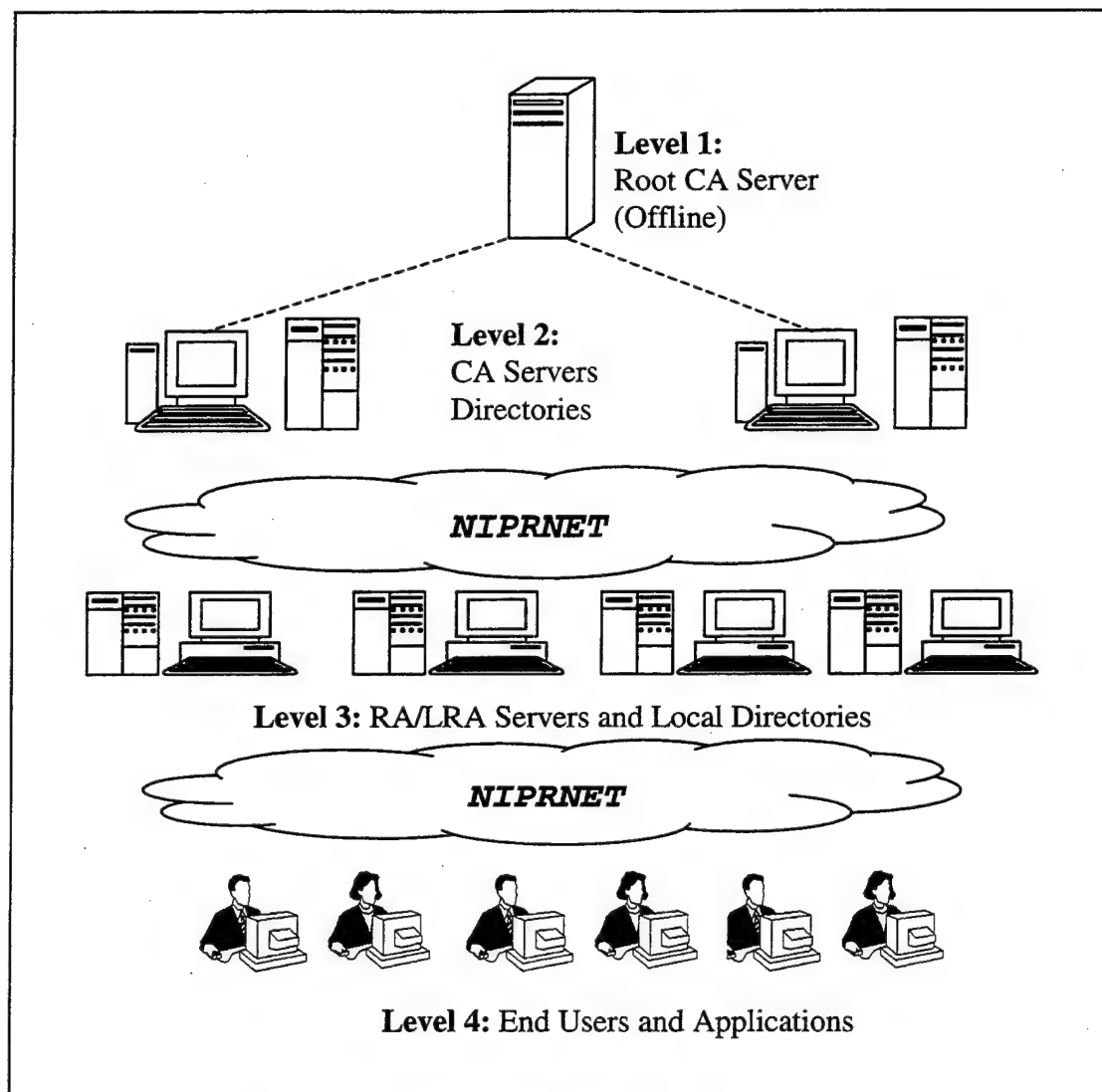


Figure 3-1. DoD PKI Organizational Levels (NIPRNET)

number of DoD CAs is expected to be a small number of regionalized sites in the continental US as well as possible sites in the Pacific and European theaters [DOD99]. For the protection of sensitive but unclassified (SBU) information (e.g., mission support, administrative, and format sensitive), the outsourcing of PKI services to commercial service providers is a viable option. However, these outsourced PKI services must meet the security and functional requirements mandated by the DoD PKI. Studies must also be

conducted to determine whether outsourcing will be the most cost effective choice for the long-term operation of PKI services.

Within the certificate management context, the DoD PKI Directory Services will consist of directories and databases that serve as a repositories and subsequent distribution points for DoD digital certificates and Certificate Revocation Lists (CRL) [DOD99]. Other relevant information, such as email address, unit postal addresses, and phone numbers, may also be maintained and distributed via the directories. Users may access the DoD PKI Directory Services through a web-based interface to download certificates or retrieve information about other users. The DoD objective is to establish a common DoD-wide directory to support all DoD public key enabled applications [DODb99].

Local Registration Authorities (LRA) and Local Directory Services represent the third level of the DoD PKI. DoD components, services, and agencies may opt to operate one or more Registration Authorities (RA) to establish and oversee the operations of their respective LRAs. LRAs consist of personnel certified and trained by a DoD CA or RA, plus registration workstations running software to interface with a DoD CA. Local directories will be extensions of the centralized DoD common Directory Services and may be utilized to support local operations and enhance performance [DOD99a]. Local directories may also enhance performance and alleviate congestion at network points of presence by reducing the frequency of queries from local applications back to the centralized Directory Services. However, the advantages of local directories may be offset by delayed directory updates and untimely CRL information.

The fourth level of the DoD PKI consists of end users and applications. End users are responsible for registering in person with an LRA and protecting their private keys from disclosure. End users may wish to back up their private keys to ensure continued access to their data. However, in the event that a private key is lost or compromised, the owning user must immediately notify the issuing CA so that the associated certificate can be revoked and the revocation can be published in the CRL. PKI enabled applications will interface with the DoD PKI to obtain digital certificates, verify certification paths, and check revocation information such as CRLs. Applications will rely heavily on the Directory Services to perform these functions.

As mentioned, the NSA owns and operates the Root CA and is, therefore, primarily responsible for Level 1 services. The NSA is also responsible for the DoD PKI program management, with the Defense Information Services Agency (DISA) serving as the Deputy Program Manager [DOD99]. DISA is currently providing certificate management (Level 2) services as part of a DoD Medium Assurance PKI Pilot. This pilot will be transitioned into the Class 3 DoD PKI, while the FORTEZZA-based PKI effort supporting the Defense Message System (DMS) will transition into the Class 4 DoD PKI [DOD99a]. Assurance levels and the corresponding certificate classes are discussed in the next section. As the DoD PKI continues to evolve, some Level 2 services could be outsourced, while others could become the responsibility of other DoD components or tactical forces. Level 3 and 4 services will primarily be the responsibility of DoD CINCS, services, and agencies; however, outsourcing may also be considered for registration

services and local directory services involved with the protection of sensitive, but unclassified information.

### **3. Assurance Levels and Certificate Types**

The level of assurance of a public key certificate is the degree of confidence in the binding of an end user's identity to the public key pair. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a CA [DOD98]. The DoD PKI will support three levels of information assurance, defined as Classes 3 and 4 for the protection of unclassified/sensitive information, and Class 5 for the protection of classified information on open networks (unencrypted) or other high-risk environments. To ensure consistent use of the certificate classes throughout the DoD, the DoD X.509 Certificate Policy describes each certificate class and provides basic guidance for its use [DOD98]. The DoD PKI will be capable of issuing a corresponding class of certificates to meet the requirements of each assurance level.

Class 3 certificates are designed for applications handling low to medium value information in a low to medium risk environment, such as business transactions or SBU administrative information over open networks [DOD99a]. Class 4 certificates are intended for applications handling medium to high value information in any environment, such as SBU mission critical information in a high-risk environment. Class 5 certificates will be used for applications handling classified information in a high-risk environment such as the NIPRNET or other open networks.



Within each of the certificate assurance classifications, the DoD PKI will issue two different types of certificates based on functionality: identity certificates and encryption certificates. Each type will have a common set of attributes so that certificates will be standard throughout the DoD [DOD99]. Identity certificates will be used for authentication of a certificate owner across networks and for non-repudiation. Non-repudiation requires that the private key remain under the owner's exclusive control; therefore the private keys associated with identity certificates may not be escrowed for key recovery. Encryption certificates will be used to encrypt information for confidentiality. The private keys associated with encryption certificates may be escrowed for key and data recovery. Certificates may be issued to personnel or to equipment, such as servers, routers, and other network communication equipment.

### **C. MARINE CORPS ROLES AND RESPONSIBILITIES**

This section consists of recommendations for establishing roles and responsibilities within the Marine Corps for developing and implementing a PKI. As stated in the DoD PKI Implementation Plan [DOD99a], the Marine Corps will:

[...] identify PKI-relevant operational requirements and review and participate in technical and programmatic planning activities associated with the execution of the DoD PKI. [The Marine Corps] will procure PKI and PKI-enabled technology consistent with the DoD PKI Roadmap and appropriate standards, and deploy and sustain day-to-day PKI operations.

The Headquarters Marine Corps (HQMC) Assistant Chief of Staff (ACS) for Command, Control, Communications, Computers, and Intelligence (C4I) should assume overall

responsibility for planning, directing, and coordinating USMC PKI efforts and should direct the establishment of a formal USMC PKI Program. ACS C4I should serve as the USMC PKI Program Sponsor and, in this capacity, be the center of PKI policy, standards oversight, and systems integration for the Marine Corps. All PKI efforts within the Marine Corps should be coordinated through and authorized by ACS C4I. Application-specific PKI implementations not authorized by the official USMC PKI Program should be discontinued.

As the program sponsor, ACS C4I should prepare a Joint Operational Requirements Document (ORD) and provide it to the Marine Corps Combat Development Command (MCCDC). The Joint ORD should describe the operational requirements for a DoD and USMC PKI based on unmet deficiencies for information protection and IA. MCCDC should then develop formal requirements based on the information identified by ACS C4I in the Joint ORD. The formal requirements for a USMC PKI should then be validated through MCCDC's Combat Development Process to ensure that they support current doctrine, adhere to approved standards, and comply with the Commandant's Planning Guidance and the Marine Corps Master Plan [MCCDC99]. Upon completion of requirements validation, a USMC PKI Initiative can be submitted to the Program Objective Memorandum (POM) Working Group for consideration in the FY-02 POM. An approved requirement officially begins the acquisition process.

Marine Corps System Command (MARCORSSYSCOM) should be designated as the USMC PKI Program Management Office (PMO) and, therefore, would be responsible for overall program management and acquisition of the USMC PKI. The USMC PKI

PMO should coordinate closely with the DoD PKI PMO to ensure consistency and alignment with DoD policies, procedures, standards, and practices. Additionally, the USMC PKI PMO should communicate frequently with ACS C4I to ensure that the program continues to meet the objectives and requirements of the overall USMC PKI effort, as well as USMC IA efforts. Based on the DoD and USMC PKI Roadmaps, a program strategy should be developed, including a project timeline, as well as a resource strategy identifying required program resources and any resources of existing programs that may be sourced for PKI development purposes (e.g., EKMS and DMS). MARCORSYSCOM should also identify other programmed systems that will require PKI services and ensure that existing public key mechanisms are in compliance with current DoD standards or that compatible public key mechanisms are integrated into each system's development process.

The USMC Network Operations Center (NOC) is responsible for the overall management, operation, and maintenance of the Marine Corps Enterprise Network (MCEN) and, in that capacity, should be responsible for implementing and maintaining the infrastructure supporting the USMC PKI. The USMC NOC is currently operating an RA and LRA as part of the DoD Medium Assurance PKI Pilot. As the DoD Pilot makes the transition into a Class 3 DoD PKI, the USMC NOC RA should also make the transition to provide Class 3 services. Additionally, the NOC RA should integrate Class 4 services to support the migration of all systems from Class 3 to Class 4 by December 31, 2002 [DSD99]. As the USMC RA, the NOC will be responsible for establishing, registering, training, and overseeing USMC LRAs supporting Class 3 and Class 4

services. The LRA at the NOC should initially serve as the sole USMC LRA for the National Capital Region (NCR). As the PKI evolves, additional LRAs may be established as necessary to support the NCR. A backup RA will be established in Kansas City, Missouri.

#### **D. USMC PKI OBJECTIVES**

The foundation for secure Internet, NIPRNET, and intranet distributed applications for the Marine Corps is an enterprise-wide PKI solution. The target USMC PKI should be developed as an integral component of the Marine Corps Enterprise Network and, as such, should constitute the core of the USMC's overall network security infrastructure and IA capabilities. The USMC PKI should be developed in accordance with the DoD PKI Roadmap, with the specific objective of meeting DoD's intent in a timely, responsible manner. The elements of the USMC PKI will be integrated components of the DoD PKI and will eventually support a broad range of joint and USMC security-enabled applications. Secure interoperability across the Marine Corps and within the DON and DOD is paramount to Marine Corps internal and joint operations.

##### **1. Certificate Management**

As described in Chapter II and the DoD PKI Roadmap, DoD CAs and Directory Services will centrally provide certificate management services. The DoD PKI is responsible for DoD-wide PKI issues such as interoperability and cross certification with other federal agencies, allies, and commercial partners; scalability of certificate management functions supporting the DoD; directory integration across the DoD;

certificate revocation and verification processes and procedures; and centralized DoD key escrow mechanisms and policies. Marine Corps developers must understand the significance of issues associated with each of these components and their applicability to USMC PKI operations.

To date, DoD PKI efforts have focused primarily on garrison infrastructure issues, with little emphasis on tactical operations and concerns. While the DoD Roadmap suggests that the target DoD PKI may be able to support tactical requirements, it also acknowledges that tactical environments may not always provide easy access to the certificate management elements and that services requiring such access may suffer. Deployed users and applications would need to "reach back" for PKI services. Reaching back from a deployed network usually involves a digital transaction from the local tactical network, across a satellite link connecting into a Standardized Tactical Entry Point (STEP) to the Defense Information System Network (DISN), and across the DISN to the network hosting the Regional CA (and back again). Due to bandwidth constraints, network bottlenecks, and multiple points of potential network failures, it may not be tactically feasible to rely on remote CAs for certificate management services.

The issuing, downloading, revoking, and verification of certificates may be accomplished more efficiently and expediently by deployed tactical CAs. If this service is not provided by the DoD PKI or by possible CINC-level solutions, then the individual services may need to acquire the resources to perform tactical certificate management services. Consequently, the Marine Corps should examine the possibility of deploying certificate management services in the form of tactical CAs, established as subordinates

to regional DoD CAs, for the duration of large deployments, operations, or contingencies. The tactical certificate management services should include the necessary directories and certificate issuance, distribution, and verification services to minimize the requirement to "reach back" for required support.

## **2. Registration**

Marine Corps registration services provide users and applications access to the DoD PKI by acting as interfaces to DoD CAs for the purposes of identity verification and certificate issuance. Registration components (RAs and LRAs) represent the core of the USMC PKI infrastructure. All PKI users must physically visit an LRA to initiate the registration process. The USMC NOC RA will serve as the central authority for Marine Corps registration policy and operations for Class 3 and Class 4 services. Class 5 services will be provided by conventional NSA-approved Type I cryptography and EKMS key distribution services until such a time that an acceptable, NSA-approved public key technology emerges [DOD99].

Consistent with the DoD PKI Roadmap, USMC LRAs will be comprised of common registration workstations with unified ordering and delivery software based on commercial standards and technologies. The LRA workstations will operate and interface with a common set of processes and tools so that the only differences between assurance levels from LRA and user perspectives are the user identification procedures and tokens protecting the keys [DOD99]. DoD envisions that a single LRA workstation will be able to transparently register users into DoD CA Servers, commercial certificate

service providers, or other external CAs as needed. Figure 3-2 illustrates DoD's target registration process for USMC users.

The primary objective of the Marine Corps registration infrastructure is to provide convenient and localized registration services with minimal cost in terms of equipment, operational funding, and manpower. LRAs must be geographically located to serve as

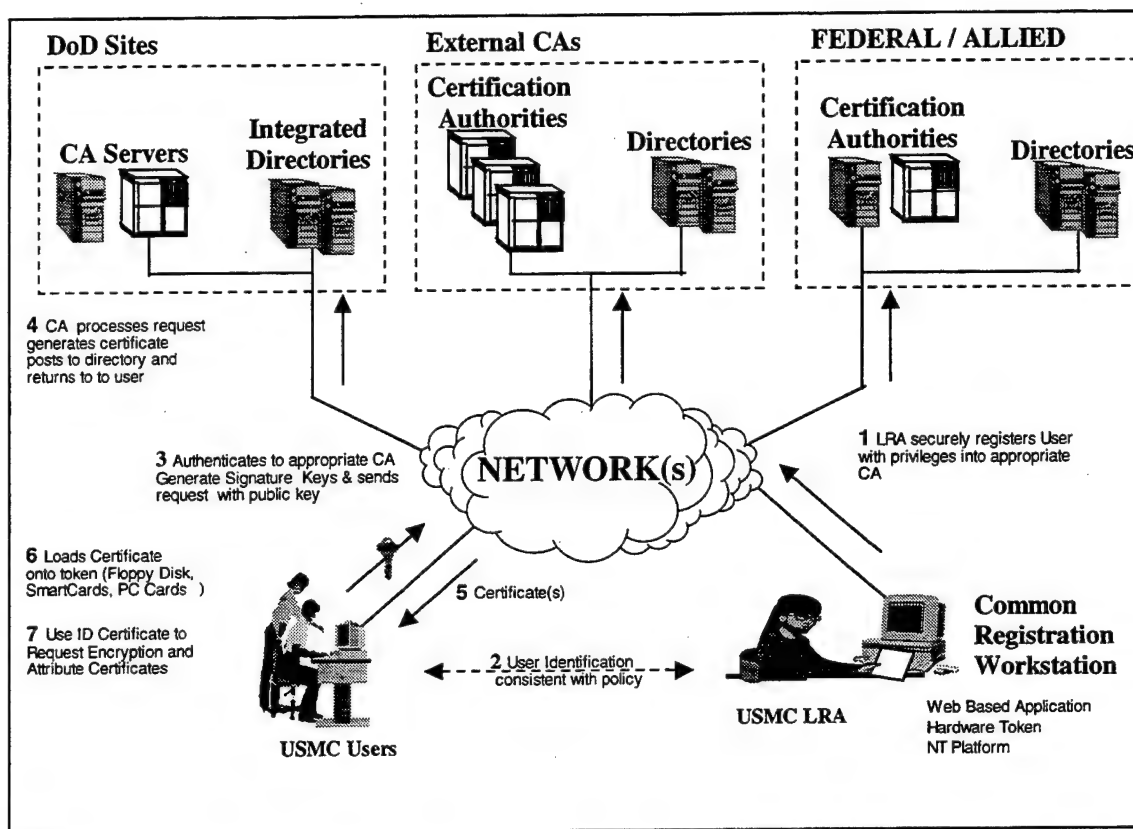


Figure 3-2. DoD Target User Registration (USMC) [DOD99]

many Marines and civilian employees as possible, while minimizing travel distances for customers and lengthy registration processing delays due to equipment deficiencies or excessively large customer-bases per LRA. The outsourcing of registration services

should be examined closely to determine the cost effectiveness of contracting the service to a commercial provider or by hiring and training DoD civilian employees to perform the registration functions. When exploring outsourcing options, manpower considerations must be weighed to determine Marine Corps costs in terms of personnel required to operate LRAs.

A second objective of USMC registration is to keep the process as simple as possible, leaving little room for errors that could result in registration failures and unnecessary re-registrations. Much of the initial complexity will result from the lack of user awareness and understanding of public key mechanisms and the supporting PKI. Training should be provided as part of the Marine Corps' IA training program to familiarize users with the basic concepts of public key cryptography and with the user registration process. A couple of options are available to simplify the registration process.

One option is for first time subscribers to complete the entire registration process, to include key generation and certificate issuance, at the LRA workstation. This could prevent the potential problems users may encounter when attempting to complete the registration process on their own from registration information and instructions received from the LRA. (See Figure 3-2). By remaining with the LRA during the remainder of the registration process, users can complete the registration process without delay, while relying on the training of the LRA to ensure the process is completed correctly. Although completing the registration process in this manner will increase the amount of time each user must spend with an LRA, registration efficiency is likely to be improved and users



will be provided with one-on-one training during the registration process. Eventually users will become more familiar with the process and may no longer need to rely on the LRA for end-to-end registration. Beyond initial registration, users may be afforded the option of completing the registration process on their own, although they still must physically pre-register with an LRA.

If this proves to be too costly in terms of time and manpower at the LRAs, a second option is to focus more on unit training and web-based directions. Unit representatives could receive training provided by LRAs and, in turn, provide that training at the unit level before registration. Implicit web-based directions could also be developed to take new users through the process step-by-step. Additionally, LRA help desks could be established to answer user questions regarding the use and handling of their keys without having to return to the LRA for assistance.

### **3. Local Directories**

Marine Corps owned and operated directories are necessary to distribute information and certificates from DoD's centralized directories to localized regions within the MCEN. Regionalized repositories of CRLs and commonly utilized certificates can reduce network traffic across the MCEN and through points of presence to the DISN backbone. However, local directories will require scheduled updates from DoD Directory Services to ensure the accuracy of the certificate information. Determining the length of time between updates is a trade off between the utilization of network bandwidth and the accuracy of directory information. Update schedules will be dependent upon the information assurance level supported by the directory, as well as network traffic patterns

and bandwidth constraints during certain periods of the day. Additionally, Marine Corps developers must ensure that local directories are fully integrated and interoperable with DoD directories systems, which are being designed to allow multiple communication options and client access protocols [DOD99]. Directory technologies must also have assurance mechanisms to protect the accuracy and integrity of the information stored within the directory itself. See Chapter IV for a further discussion of directories.

#### **4. Applications**

Marine Corps networks are populated by a variety of the Marine Corps' departmental and enterprise-wide applications and joint applications. Several emerging joint applications are being developed and fielded with integrated public key mechanisms and PKI interfaces. Examples include Electronic Document Access (EDA), Defense Travel System (DTS), and Joint Computer Aided Acquisition Logistical Support (JCAALS). Legacy applications that are not PKI-enabled may require modifications, work-a-rounds, or replacement. Future systems and systems currently in development need to include PKI planning throughout the development process and should fully incorporate public key capabilities into their designs. PKI, as well as other IA and computer security measures, must become an essential element of system design from beginning to end. Application developers must understand and be able to apply the supporting PKI infrastructure's policies, usage, and interfaces in order to effectively utilize the technology [DOD99]. To support this objective and to ultimately save money, resources, and time, MARCORSYSCOM should immediately establish a PKI section to develop Marine Corps PKI elements, as well as assist other system developers with PKI issues.

## **E. USMC PKI DEVELOPMENT RISKS AND INITIAL STRATEGY**

Recognizing the immaturity of commercial PKI products, standards, and protocols, the DoD has adopted an evolutionary approach to achieving the target DoD PKI [DOD99]. The Marine Corps must also embrace an evolutionary approach based on emerging commercial standards, in addition to establishing a development schedule based on the Deputy Secretary of Defense's (DSD) Memorandum dated 9 May 1999 [DSD99]. This has led to some contradiction between the DSD's aggressive timeline and the DoD Roadmap's cautious, evolutionary approach. Consequently, the Marine Corps must move ahead aggressively to meet the intent of the DSD's timeline while at the same time circumventing the potential risks described in the DoD PKI Roadmap.

To meet the objectives of an evolutionary approach to development, the Marine Corps must avoid the pitfalls of aggressively acquiring and implementing vendor-specific product solutions based on still immature technological standards. Although some commercial PKI solutions appear to offer nearly unlimited potential for ensuring authenticated, non-repudiable, and confidential communications across and between large, distributed networks, in addition to promises of market-wide interoperability based on the specification of recommended standards, the Marine Corps must proceed with caution. Commercial public key technology, PKI solutions, and application standards are fluctuating and evolving within a very volatile market. These factors lead to the increased technical risk that the DoD PKI will not be able to meet its operational, budget, or schedule requirements [DOD99]. Working within a limited and constrained budget, the Marine Corps cannot afford costly investments into commercial product lines that

later prove to be incompatible or non-interoperable with the DoD PKI, as well as Department of Navy (DON) PKI measures. The Marine Corps must, therefore, closely monitor the evolution of the DoD PKI to ensure strict compliance with all standards, products, and applications. Furthermore, the Marine Corps should avoid substantial investments in products or solutions supported by the DoD PKI until it has been determined that the DoD will not reverse course or change direction in favor of a different and possibly incompatible solution.

Strict compliance with the established DoD PKI standards may not be sufficient to guarantee compatibility. Although a vendor may claim that its product supports the DoD standards, product-specific interpretations of commercial standards may still result in noninteroperability between different products based on the same standards. Due to the lack of accepted PKI standards and resulting product-specific solutions tailored to market niches, none of the PKI applications currently available on the commercial market fully supports the broad applicability of the DoD PKI requirements [DOD99]. The Marine Corps must ensure that it does not fall victim to a vendor solution that does not fully address and meet the full requirements of the DoD PKI. Testing to validate that commercial products meet the full criteria of requirements for compatibility with the DoD PKI must be performed by NSA, or a commercial test facility that has been accredited by NSA and the National Institute of Science and Technology (NIST) [DOD99].

Considering these risks, how should the Marine Corps proceed to meet the intent of the DSD's timeline? Initial Marine Corps efforts must focus on developing a vendor-independent architecture based on DoD recommendations and standards guidance. The

PKI architecture must be developed within the framework of the Marine Corps' overall MCEN architectural design, including the Marine Corps IA and defense-in-depth security implementations. The PKI architecture development should consider each component and layer of the overall MCEN architecture and design, rather than zeroing in on application layer implementations. Once the PKI architecture has been integrated within the MCEN architecture, commercial implementations or outsourcing options may be considered. However, any solution must work within the framework of the established PKI architecture.

#### **F. USMC DEVELOPMENT PROCESS**

As emphasized throughout this chapter, the Marine Corps must embrace an evolutionary strategy of PKI development. Each phase should consist of a careful analysis of potential risks, followed by incremental steps towards well-defined objectives. Creating an overall system design and architecture is crucial for defining the objectives of each phase of implementation. A development process must be formalized and executed to ensure that efforts remain focused and risks are minimized. The process outlined below is a variation of a process created by a Department of Energy (DOE) team tasked with developing a security-enhanced manufacturing infrastructure (including a PKI) for the DOE's Nuclear Weapon Complex [Des97]. The Marine Corps should utilize a similar process for developing its own PKI.

##### **1. Conduct a USMC-Wide Survey.**

A comprehensive survey of all Marine Corps organizations must be conducted to determine what network applications require PKI services, what applications not

currently connected to networks may be network-enabled as a result of PKI services (e.g., applications that normally require in-person identity authentication), and what, (if any) PKI applications are currently in use. This includes other security systems and networking components that may utilize PKI services for key distribution, authentication, or access control. System incompatibilities must be identified, including legacy and stovepipe systems that may not readily support PKI-enabled applications and services. Potential resources such as smart cards, smart card readers, existing directory services, and related systems (i.e., DMS components) must also be identified and categorized (see Chapter IV for a further discussion of smart card technologies and directory systems). The primary objective of this phase is to gather the necessary information to formalize the requirements for a USMC PKI.

## **2. Develop a Basic Design**

With the results from the survey, a basic system design should be developed that meets as many of the requirements as possible. An architectural framework should be formulated that fits within the established network architecture. For instance, the MCEN security architecture must be closely examined so that PKI components and applications may be cohesively integrated with existing components, such as firewalls, intrusion detection systems, virtual private networks, and symmetric cryptographic systems. For mission-critical legacy systems not compatible with public key-enabled systems, work-arounds must be considered until such a time that these systems can be upgraded or replaced. The system design must be based on an open-architecture approach to ensure that it is accessible by a broad range of applications and implementations. Specific

considerations for designing a basic PKI architecture include: the identification of LRA locations, the availability and distribution of compatible WWW browsers, smart cards, and readers, and the distribution of the necessary LRA workstations for user registration.

### **3. Evaluate Options**

Next, an evaluation of commercial products and insourcing/outourcing options should be performed to determine how well existing solutions met the Marine Corps' requirements. As discussed earlier in this chapter, any commercial products considered must be in compliance with the standards outlined by the DoD and tested for compatibility with the DoD PKI by NSA and/or the NIST. Studies may be necessary to determine if it is more cost effective to outsource certain functions or to develop them internally based on COTS implementations. The studies must also include any potential security risks resulting from outsourcing options. The pros and cons of each option must be documented and weighted to determine an overall evaluation for each potential solution. At the end of this phase, developers should be able to answer the question, "How well does solution xyz meet the Marine Corps requirements for a PKI?"

### **4. Source and Deploy Infrastructure Components**

Next, the Marine Corps should begin to incrementally establish the PKI architecture. LRAs should be established and the appropriate equipment should be acquired and distributed. Personnel need to be identified to operate the LRAs and the necessary training should begin. Policies and procedures must be developed and practiced. Deficiencies and limitations must be identified and corrected. The overall objective of this phase is to establish a Marine Corps-wide, vendor-independent

architecture that is capable of supporting a broad range of COTS solutions and software implementations. The concept is to develop a framework to support PKI services rather than building an architecture around a specific implementation.

## **5. Re-Evaluate PKI Solutions**

After the architecture has been established, the most promising solutions and options evaluated in Phase 3 should be re-evaluated in the context of the existing PKI architecture. By this time, ongoing DoD efforts to work with vendors and standards committees to improve interoperability may have paid off. The result is likely to be a more stable PKI market with better defined standards. Depending upon DoD development efforts, the Marine Corps may choose to implement a DoD-common solution or a DoD compatible solution that more adequately meets Marine Corps-specific requirements. Evaluation must be continuous and thorough to improve upon any weaknesses or shortcomings and to prevent the implementation of a PKI solution that leads to future non-interoperability. The procurement and deployment of a particular COTS PKI solution should only be considered following a careful analysis of standard specifications, interoperability and functionality issues, and vendor-specific product claims.

## **G. CONCLUSION**

This chapter has described the Marine Corps' role within the DoD's overall IA initiatives and PKI development efforts. Marine Corps-specific responsibilities and objectives for the development of USMC PKI elements were outlined and discussed. A Marine Corps development framework was presented, including a brief discussion of



potential risks and pitfalls. The need to focus initial development efforts on architectural design rather than application layer solutions was established. A PKI development process was presented, outlining the steps for an incremental, evolutionary development approach. Technological risks and challenges are further discussed in Chapter IV.

## **IV. TECHNICAL CHALLENGES**

### **A. INTRODUCTION**

Successful implementation of the DoD target PKI hinges on the availability of acceptable COTS products and services [DOD99]. Since public key technology is immature and evolving, DoD faces technical risks that may impact its implementation timeline and affect its budgeted costs [DOD99]. Many of these risks will apply directly to Marine Corps development efforts and, therefore, must be fully understood and considered by Marine Corps developers. None of the PKI-enabling products currently on the market fully support the target DoD (and subsequently the Marine Corps) PKI requirements [DOD99]. Lack of accepted PKI standards and protocols in industry has resulted in product-specific solutions, tailored to narrowly focused markets. This trend in industry has hampered DoD's objective to create a standards-based, vendor-independent PKI solution.

The purpose of this chapter is to identify major technical challenges in the development and implementation of the Marine Corps PKI. Discussions will include technical challenges surrounding directory services, key escrow, and smart card technology, emphasizing critical interoperability and scalability issues for these components. System scalability is a requirement for PKI components in supporting a growing number of users and applications. Additionally, components must be interoperable with other PKI components both within the Marine Corps Enterprise Network (MCEN) and the greater DoD enterprise network. In defining the challenges

and describing their potential impact on the Marine Corps PKI, this chapter will address the technical risks for the Marine Corps and recommend courses of action to optimize interoperability and scalability.

## **B. DIRECTORIES**

Directories will play a significant role in the development of an enterprise-wide PKI implementation. For this reason a discussion of their functions, alternative technologies, capabilities and limitations is appropriate.

### **1. Definition of a Directory**

A directory is a network resource that identifies all resources on a network. When client programs contain application-programming interfaces (API's) written to access these information repositories, directories facilitate access to network resources by users and applications. Network resources may include e-mail addresses, white page information, computers, peripheral devices, digital certificates, etc., [Web99]. For example, using a directory-enabled e-mail application, a user can search the directory for the e-mail address of his intended recipient, and select it as the addressee in his mail message. Additionally, a user can locate the digital certificate of a communication partner for use in a confidential message or may use the certificate for authentication and non-repudiation services applied to received mail. The directory service facilitates the search for and access to the certificate by the user's application.

### **2. Purposes of Directories**

In the context of a PKI, directory services provide an essential mechanism for the storage and distribution of digital certificates and their associated public keys, as well as

white page information. A directory service also provides convenience and efficiency for enterprise network users whose network is distributed over a number of geographic locations. Through replication techniques, directory servers can compare and exchange information to provide users and applications easy access to current directory information [ICLM97].

As mentioned above, the purpose of directories is to provide a convenient and easily accessed repository from which users and applications can obtain digital certificates and certificate revocation information. As discussed in Chapter II, Certificate Revocation Lists (CRLs) provide one way to identify certificates that have been compromised or withdrawn [ICLP97]. Recall from Chapter II that a PKI is deployed to establish a network of trust, enabling a public key system to provide true authentication and non-repudiation services. By posting certificates and revocation information in CRLs to directories or requiring lookup of certificates in a directory, an organization can improve its network security and level of trust as user's and applications will be able to verify the status of certificates they want to use in confidential communications. Since certificates are instruments of trust, directories distribute that trust among and within PKIs. Thus, by conveying trust, directories allow users and applications to find information and certificates for entities with whom they want to establish trust relationships and to verify the validity of those certificates. Providing these services is critical for sustaining user confidence in the PKI's level of trust.

The contents of directories should be controlled by access controls. Each organization has a security policy with regard to information. Access controls applied to

directories represent an implementation of those security policies. The directory service should provide flexibility in the application of access control mechanisms. For example, the Marine Corps may want to provide universal access to some of its directory information by authorized Marine Corps PKI users. Thus, all authorized users could be allowed to read the information. Yet, the Marine Corps may want to use some directories to provide access to restricted information, requiring that their contents are known only by select users. For example, through a web browser, authorized Marines could authenticate themselves to the restricted directory server by providing their digital certificate. Using the certificate information provided by the Marine requesting access, the directory server would compare the digital certificate to a database containing certificate information of authorized directory users. Thus, the directory access controls determine who can browse the contents of the restricted directory.

User access issues involve the choice of access protocols used (X.500 or LDAP v.3) and security issues such as the means of controlling access to the information in the directory [DOD99]. Directories can store attributes such as permissions, access levels, and role-based rules that determine the access level users and applications have to directory resources [Gar99]. For example, Marines could use digital certificates to gain access to a directory from a web browser. The certificate can be used in part of an authentication protocol between the client and the server. A valid certificate (obtained through proper authorities) would provide access to the directory.

Directories can facilitate access to a wide variety of information in various formats. By connecting to different databases, directories can provide embedded

documents, presentations and Uniform Resource Locators (URL's)--the addresses used on the World Wide Web [How99]. As mentioned earlier, directories can be used for e-mail purposes or as a human resource database. For example, directories can list "white" and "yellow" pages, providing information on individuals and organizations such as e-mail addresses, phone numbers, postal addresses, etc. [DOD99].

Thus, PKI directories, by design, are distributed name services, providing repositories for digital certificate information and certificate storage. The directory service allows applications and users to locate the resources they need and are a critical enabler for the success of a PKI in the enterprise. Ideally, directory services will make the physical network topology and protocols transparent, so that the users can access any resource without knowing where or how it is physically connected.

Carefully developing and implementing a distributed directory system based on common standards and protocols such as X.500 and LDAP v.3, and synchronizing directory information through metadirectory technology make seamless directory services possible. To illustrate this, an entry (say, Capt I.M. Smith) is posted on a directory containing attributes that represent this Marine. The attributes may include Captain Smith's digital certificate or white page information about him such as his organization, phone number, e-mail address and billet. Once posted on the directory, users and applications within the Marine Corps PKI (or the greater DoD enterprise network, if configured for this) can access the entry using open protocols such as X.500 or LDAP.

Consider the number of users who could potentially require access to that entry. To avoid a bottleneck at a single directory server, directory entries should be replicated to

multiple directory servers. These servers should be carefully placed throughout the organization to provide optimal support in terms of the number of PKI users, bandwidth and infrastructure requirements. Thus, the overall directory structure is distributed throughout the organization. Through metadirectory technology, directories can synchronize distribution of digital certificates, white page information and CRLs to other directory servers in the PKI, making these resources available from any computer within the PKI. Additionally, with the emergence of the X.509 v.3 standard, directories and databases of any type can be used to store and allow access to certificates and the public keys they contain [Gar99]. These are a few examples of the directory's purpose.

### **3. Approaches to Directory Service Standards**

There are two perspectives to directory services: user access and administration. User access issues involve the choice of access protocols used such as X.500 or LDAP v.3 and also security issues such as the means of controlling access to the information in the directory [DOD99]. Administration involves managing the directory system through server-to-server connections. Administration includes management of the information contained within the directory information base [DOD99]. The following sections will address the user and administration perspectives by comparing and contrasting X.500 and LDAP, defining their uses and highlighting their relative strengths for providing directory services in an enterprise network.

### **4. Directory Service Technology**

In choosing a directory system, the Marine Corps will want a product that both integrates quickly with existing infrastructure and is easily deployed. In keeping with the

Marine Corps' expeditionary character, directory servers should have the flexibility to deploy in a vendor-neutral environment, saving time and cost for work-arounds or middleware and providing the potential for interoperability in a joint or multi-national environment. Additionally, the Marine Corps should consider directory solutions that provide lower cost of ownership, including purchase price, maintenance, upgrades, and administrator training.

Two of the directory service standards currently available include X.500 and LDAP v.3.

*a) X.500*

The X.500 standard defines models for a highly distributed database, designed as a repository of information facilitating communications [Chad99]. X.500 is the common model for all directory systems and thereby provides the potential for connecting various COTS directory systems into an enterprise directory service. Thus, all proprietary variations for directory architectures are based on this model (i.e., Netscape Directory Services, Microsoft Exchange, Banyan Streetwork, etc.) [ICL99M].

As the Marine Corps is planning a distributed PKI directory system, X.500 offers the opportunity to join disparate servers in a unified directory repository. X.500 systems are standardized open services and protocols that provide for sophisticated, distributed data access and also replication of data between servers and directory systems [ICLM99]. Through these capabilities, X.500 systems can broaden the reach of the infrastructure and its users by promoting interoperability and the open exchange of information throughout the Marine Corps and the DoD.



Although COTS products for directory services apply the X.500 model's naming and functionality specifications, few if any vendors comply with it fully, because the standard is so complex [Web99]. By adding their own proprietary fields to the naming specifications, vendors create interoperability problems among products in the directory service market. In addition to its inherent complexity and cumbersome overhead, X.500 has several drawbacks. First, since it was not designed for Internet use, X.500 does not provide confidentiality protections like Secure Sockets Layer [How99]. Therefore, by itself, X.500 directory service will not easily provide access to remote access users dialing into the Marine Corps Enterprise Network (MCEN) via the Internet. Second, X.500 does not support directory services for listing Uniform Resource Locators (URL's). Increasing the potential for complex workarounds, X.500 does not support standard Application-Programming Interfaces (API's) or standard data formats which detail how software programs access the directory and supply a standard set of function calls and definitions [How99].

When implementing an enterprise-wide directory service, the Marine Corps should consider the advantages provided by X.500's standard server-to-server protocols, including DSP, DISP, DOP, and BAC. Directory System Protocol (DSP) is used for chaining requests in server-to-server communications [How99]. For example, a user needs access to another Marine's digital certificate. The user types the Marines last name at the directory search prompt. Although the local directory server may not list the Marine's certificate, it can query other directory servers on the network for this information and return it to the requesting user. Thus, DSP hides the complexity of these

server interactions from the user, so the user can access the information within the directory without needing to know the exact location of the information [Shu99]. Through DSP, X.500 enables the user to perform fast and efficient searches of directory information in a seamless manner [Shu99].

To provide convenience to the user, the Marine Corps should minimize access times for directory information. Maintaining information “near” the users who need it can do this. Directory replication enables the information to be copied to multiple directories, reducing access times. DISP, the Directory Information Shadowing Protocol, allows one directory (a supplier) to provide another (a consumer) some or all of its directory information and then keeps the consumer informed of any changes occurring to that information [Ste97]. This process is called shadowing. With this protocol, directory information can be managed centrally and then replicated to other directory servers, saving much time and effort for the administrator. DOP, X.500’s Directory Operation binding Protocol, is used for negotiating replication agreements between servers [How99].

Finally, since directories enable an organization’s information to be both widely distributed and widely available, access to this information must be controlled [Ste97]. For directory security, Basic Access Control (BAC) specifies a standard access control scheme, determining what users or applications can access the directory information [How99].

*b) LDAP*

Based on the standards contained in X.500, the Lightweight Directory Access Protocol (LDAP) is a set of protocols for accessing information directories [Web99]. LDAP was initially designed to be a low-cost, PC-based front-end for accessing X.500 directories. [How99]. Created for network layer access, LDAP supports TCP/IP and is quickly becoming a de facto Internet standard for directory services [Web99]. Although not yet widely implemented, LDAP offers the promise that virtually any application on almost any computer platform can obtain directory information such as e-mail addresses and digital certificates [Web99]. As LDAP is a standards-based, open protocol, applications need not worry about the type of server operating system hosting the directory [Web99].

LDAP itself is also a repository for storing directory information and digital certificates and can thus function as a stand-alone or distributed directory service alternative to X.500. As a repository of directory information, LDAP can facilitate flexible, centralized digital certificate management. System administrators can store much of the information required to manage certificates in an LDAP-compliant directory [NetD99]. For example, a CA can use information in a directory to pre-populate a certificate with a new Marine's name, billet description, and other identification information [NetD99].

As a communication protocol, LDAP can be used to support the automation of routine management techniques [NetD99]. The LDAP protocol enables the CA to leverage directory information for issuing certificates in bulk or individually

[NetD99]. If keys are generated by the CA rather than at the user's browser, the CA can then distribute keys to a single user or to multiple users via LDAP [NetD99].

Additionally, through the LDAP protocol, applications can access directory services to check for renewed or revoked certificates in CRLs [NetD99]. With the aid of digital certificates, LDAP supports access control policies, since users or groups attempting to access directory resources via LDAP must have the appropriate digital certificate to gain access to the resource. [NetD99].

For all its touted flexibility and enabling characteristics, LDAP cannot do everything. Since it lacks the heavy update, transaction processing and reporting capabilities of a relational database, it should not be used as a replacement for systems such as an airline reservation system [How99]. Therefore, without a true relational structure or a relational query language like Structured Query Language (SQL), LDAP can not replace existing Marine Corps database management systems, built on these capabilities [How99]. Additionally, LDAP cannot serve as a file system. Based on simple pairings of attributes and values, its information model is not designed adequately to support the binary large object (BLOB) data that is normally managed by file systems [How99].

Another drawback is that, unlike X.500 that provides DISP and DOP, LDAP has no standard protocols for replication between multiple sites [How99]. LDAP also lacks standard access control over directory data, thus, providing no facility for ensuring that each database replica follows the same rules for access control [How99].

Work on standards for replication and access is ongoing, and specifications for these functions are expected from IETF in the near future [How99].

In spite of these drawbacks, LDAP offers the Marine Corps several advantages for providing directory access to PKI-enabled applications over the Internet. LDAP is compatible with X.500, which allows users to access directory information from an X.500 service through the LDAP protocol. In answer to the vulnerability to key compromise during transmissions over non-secure networks like the Internet, LDAP provides confidentiality protections through use of SSL, thereby enabling centralized key generation by the CA. [How99]. LDAP also supports multiple directory service protocols such as URL searches and standard API's and data formats [How99]. For these reasons, LDAP offers the opportunity for increased interoperability as will be shown in the discussion of metadirectories.

## **5. Metadirectories**

Coexistence of X.500 and LDAP may come with the development of metadirectories [Shu99]. Metadirectories are directories of directories, providing a single point of administration from which to access and update many different directories [Shu99]. Industry analysts predict that meta-directories will form an important component of a migration from proprietary and non-interoperable directory services to those that are standards-based [Shu99]. Acting as a clearinghouse for synchronizing an organization's directories, metadirectories provide a unified set of directory information by integrating information held in X.500 directories and proprietary directories such as Netscape Directory Services, Novell Directory Service and Banyan's Streetwork Directory

Service [Shu99]. Thus, the Marine Corps should evaluate metadirectories for unifying its legacy system directories with the PKI directories.

Both X.500 and LDAP have been identified as key components in the development of metadirectories. In a metadirectory model, X.500-based directories would provide the central repositories of directory information, controlling and facilitating access to data in COTS directories [Shu99]. Using the LDAP Data Interchange Format (LDIF) as the directory access protocol, LDAP could control communication from directory users, retrieving and populating the proprietary directories with the organization's core information [Shu99].

Metadirectories add value to the entire directory system by integrating the information held in multiple directories across the enterprise and then synchronizing this information for each individual item among the multiple directories. Through a combination of the LDAP communications and X.500 replication techniques discussed previously, the metadirectory can merge information about a Marine placed in different directories such as his or her e-mail address from Microsoft Exchange and his certificate from Netscape Directory Server [ICLM97]. Such features increase the completeness of the enterprise-wide directory information and reduce desktop maintenance costs through storage of configuration items that might otherwise be held in PC-based files, scripts or registries [ICLM97]. Thus, by merging directory information from directory servers spread throughout the enterprise network and by synchronizing the distribution of directory information changes, metadirectories help maintain the currency of directory information and provide a more complete picture of individual entries.

## **6. Recommendations**

### ***a) Open Standards Solutions***

According to the DoD Roadmap, the DoD target PKI directory system will allow multiple communications options and client access protocols. For the Marine Corps, the optimal method for attaining this goal is to select directory solutions that conform to the latest industry standards for directory server functions such as X.500 and LDAP v.3. The Marine Corps should not rush to buy a proprietary, non-standard PKI product and attempt to redesign its architecture around it. Re-engineering an architecture intended to conform to a particular product is usually more expensive than to engineer the desired capabilities into the architecture from the beginning. The Marine Corps should look for standards-based solutions that design their interfaces to specifications, so the organization can use any application that meets the specification and avoid vendor-dependent, stove-piped solutions. Thus, directory servers should be able to integrate a wide variety of standards-based vendor products [ICLM99].

### ***b) Simplified Management and Integration***

Optimally, quick deployment and simplified management should mark directory installation. The underlying complexity of the directory is hidden, thus providing a product that is easy to use [ICLM99]. As the number of directory servers grow, administration can become difficult if servers are not centrally managed and chosen for conformance to interfaces provided by the directory system. The directory system should smoothly integrate with existing MCEN systems, processes, and policies, giving the organization powerful in-house control of its security infrastructure [NetD99]. By

leveraging this integration, the Marine Corps can minimize ongoing system administration costs and optimize its ability to manage incremental growth [NetD99].

*c) Robust Security Mechanisms*

Directories must have strong security mechanisms providing inter-server security and strong authentication [ICLP99]. The directories themselves should easily integrate into the X.509-based security infrastructure, so that they can use the existing directory information for authenticating their server-to-server or browser-to-server interactions. According to the DoD PKI Roadmap, Secure Sockets Layer will be used to allow the directory server to authenticate itself to the client requesting information. Thus, the client, be it a user at a web browser, a PKI-enabled application, or another directory server, can know through verification of the certificate chain that the directory server being accessed possesses a certificate signed by the DoD root CA. Likewise, the client will authenticate itself to the directory server, substantiating its membership in the DoD PKI.

Some remote Marine Corps installations will connect to the Marine Corps Enterprise Network (MCEN) through non-secure environments such as the Internet. These connections will require confidentiality and create a need for network or transport layer encryption such as that used in Secure Sockets Layer (SSL) or IP Security Protocol (IPSEC). SSL facilitates the authentication procedures discussed above and also provides data confidentiality through an encrypted pipe between client and server created by the exchange of symmetric keys [DoD99]. Because SSL is merely a transport layer protocol providing authentication and session confidentiality, the Marine Corps should consider



additional security protections, depending on the information sensitivity, such as network layer encryption provided by VPNs. Additionally, once a user accesses a directory server, administrative security features, configured with digital signatures for strong authentication and identification as well as non-repudiation of administrative actions on the directories, should provide an audit trail [DOD99].

*d) Centralized Management*

Another important management consideration is the ability to administer directory servers from remote locations. Greatly simplifying an administrator's tasks, this service is called single-point administration [ICLP97]. This service provides convenience to the administrators and saves time and money in travel costs and lost productivity from administrators traveling to the problem server's location. It also provides for the centralized management and control of standard implementation procedures for ensuring consistency throughout the Marine Corps.

*e) Interoperability*

Interoperability is a critical issue for PKI-enabled technologies and represents an area of major cost if attempted in an unorganized manner [DOD99]. The DoD Program Management Office has the responsibility to ensure that the multiple directory systems within DoD are integrated into an interoperable directory infrastructure and architecture that can be used across DoD [DOD99]. Directory service interoperability is important, since users and applications will rely on the availability of certificates for their PKI-enabled communications.

As mentioned earlier, directory service vendors create interoperability problems among products in the directory service market by adding their own proprietary fields to the naming specifications. If users cannot obtain the certificates or information they need to communicate with other parties/applications, losses in productivity and missed opportunities will result. As an illustration of this issue, consider the problem caused by out of date information such as an old e-mail address. A user attempts to send e-mail to an organization for arranging a planning meeting not knowing that the e-mail address for the organization has expired. Without interoperability with the other organization's directory service, the user cannot automatically confirm the address through his e-mail application's directory. The user sends the message anyway. Some time later, the message is returned by the mail service as undeliverable. How many hours were lost that could have been used for planning the meeting?

A possible solution to the directory naming conventions issue can be found in DoD's approach to certificate attributes. According to the DoD PKI Roadmap, DoD identity certificates will have a minimum, common set of attributes (i.e., citizenship, government/non-government employee, service or agency affiliation) to establish a baseline for interoperability among service directories. Likewise, DoD should establish a baseline for directory service interoperability, requiring directory schema to have a common set of fields upon which the services can build their unique information representations.

Expired directory information frustrates users and can create serious security risks for organizations. If the Marine Corps has 60,000 e-mail users, even a one-

percent failure rate is unacceptable. Also, the support costs of tracing failed e-mail messages can spiral dramatically [ICLP99]. Security risks increase when Marines leave the service but their user accounts and passwords remain active. These accounts can be exploited by hackers looking for active but idle accounts that help hide their illicit operations. Such problems can be mitigated by maintaining interoperable directories, so that revocation information can be accessed in real time.

*f) Cross-certification*

Other interoperability problems develop in the absence of cross-certification of inter-service and inter-agency certificates. Cross-certification techniques developed by CA's allow certificates from External Certificate Authorities (ECAs) to be certified for use in the Marine Corps PKI. ECAs are Certificate Authorities from other agency or service PKIs. As the use of PKI-enabled applications grows, the Marine Corps will want to interoperate with other services and agencies. To do this, users and applications will require access to information and certificates from external directories and databases.

The Marine Corps will want to access these resources without having to develop expensive new systems. Therefore, the Marine Corps should use a common sense approach to interoperability and look for commonality and open solutions for certificate repositories. In this way future unions of PKIs (i.e. inter-agency and inter-service) can be formed to facilitate national, multi-national (NATO/inter-allied) and multi-organizational identification and communication solutions for the information societies of the future.

It should be noted that cross-certification is a NSA and DISA responsibility; however, the Marine Corps will want to remain abreast of progress made toward resolving this technical challenge. As the Marine Corps will need to fully interoperate within the DoD PKI, cross-certification will remain a concern not only for NSA and DISA, but also for all the services.

Significant issues remain when dealing with ECAs certificate revocation processes. For example inter-service CAs within the DoD PKI must coordinate the frequency of CRL publishing and directory replication to ensure the validity of certificates. Prior coordination of directory administration is imperative for maintaining a high level of trust. Obsolete CRLs degrade the trustworthiness of the directory information, reducing the level of trust for the entire PKI. Additionally, administrative procedures with external CA's must provide auditing mechanisms. Since a CA would be able to access an external CA's directory data, there must be protections in place, providing inter-server security and strong authentication to prevent unauthorized access or modification [ICLP99]. Thus, synchronization and replication of directory information such as certificates and CRLs must be closely coordinated to keep a directory system current with known compromised or withdrawn certificates [ICL]. Such issues are paramount to an organization's network security

An example of positive steps in industry toward directory interoperability is the Directory Enabled Networks initiative (DEN). Supported by numerous network software vendors, DEN is an effort to define models and schema for network-level devices and services such as routers, switches and VPNs [How99]. The schema defines

the actual data elements that can be stored in a particular directory server and how these elements relate to real world objects such as countries, organizations, individuals, and groups. Through DEN, these devices and services use LDAP to implement authentication and policy services, enabling end-to-end quality of service (QOS) [How99].

*g) Scalability*

As the size of the PKI grows to include more users, applications and directories, issues such as bandwidth and infrastructure become more important. To replicate the certificates, white page information, and CRLs in a timely manner, the PKI requires adequate throughput and processing capabilities. Poor synchronization and outdated directory information can lead to user frustration and security risks for the organization.

(1) Performance. High performance directory services are an essential ingredient of any certificate management strategy [NetD99]. "To reap the economic benefits of electronic commerce, companies must have the right infrastructure to manage the size and scope of an enterprise-wide deployment, including a public key infrastructure and a directory" [ICLP97]. It follows that, to support the requirements of a large enterprise with thousands of digital certificates, the Marine Corps' directory system must be built upon directory servers that provide sub-second response time and enterprise-wide scalability [ICLP97]. As the PKI use increases, users will continue their demands for a responsive system where certificates can be easily and rapidly accessed. To support these demands, directories will require superior processing capabilities to

integrate changes to directory information and then to replicate these changes throughout the directory system. Such performance demands require directory servers that are optimized for scalability, throughput, storage capacity, availability, and reliability.

(2) Ease of Use. Additionally, directory access procedures must be user friendly. The data must be held in a way that enables users to easily find the desired certificate or owner information, and must be structured in a standard and familiar way throughout the Marine Corps [ICLM99].

(3) Directory Service Availability. The success of PKI implementation depends on directory accessibility: having the public keys and CRLs held in a repository that all users and applications utilizing the PKI can easily access at all times. Replication—copying a directory's information to one or more directory servers--can help maintain a high level of directory information availability. For example, consider the requirement for high availability to services from a Marine Corps directory server, providing authentication services for an operation-critical Web application. If the directory server is down, the Web application cannot authenticate users, possibly threatening the success of the operation. A method for reducing risk in this situation is to create two or more copies of the directory data, each served by a separate directory server [How99]. If one copy becomes unavailable, the other can provide the service [How99]. What does this have to do with scalability? To accomplish these replication tasks without interfering with service to the users, the directory system must be scalable and responsive to the demands. The process must be transparent and seamless to the user.

(4) On-line Verification. Scalability in relation to performance requirements is particularly important when implementing on-line verification, a.k.a. real-time status checking. Due to the limitations of CRLs in providing current revocation information, the Marine Corps may find a need for real-time verification via server queries in addition to CRLs. Depending on the frequency in which an organization publishes its CRLs and the speed of directory replication, directory information may become obsolete.

Certificate verification is a critical process for maintaining a high level of trust in the PKI. In addition to publishing a CRL at regular intervals for certificate verification by users, the certificate's validity can be checked directly with the CA each time the certificate is presented for authentication [NetD99]. CRLs are maintained as a secondary verification source should connectivity to the CA be lost. In terms of scalability, consider the demands placed on a CA's server performing a single search of a multi-million-entry database to verify a certificate. Multiply this requirement by potentially thousands of users and their applications. As one can see, scalability is crucial for preventing bottlenecks and providing responsive on-line verification services.

(5) Scalability Summary. This section has shown that, if the Marine Corps is to successfully implement a distributed directory architecture, directory products should be chosen on the bases of scalability in terms of performance and reliability. The Marine Corps will want to link directory entries to non-directory data held in relational databases such as Marine Corps manpower or force structure data. To optimize user friendliness in these implementations, real-time access should be

considered. The Marine Corps should evaluate middleware, directory products, and enhancements to the MCEN infrastructure that will facilitate real time access.

### **C. APPLICATIONS**

Another key component to interoperability is the PKI-enabled applications. From the moment the Marine Corps decides to implement a PKI, the organization should strive to procure or create interoperable PKI-enabled applications. Without full interoperability, separate, technologically isolated PKI's may emerge within the Marine Corps to support specific applications. This situation becomes prohibitively expensive, when attempting to re-engineer interoperability where it was not initially designed [ICLP97]. In addition, these PKI islands create user confusion and frustration, since users will be required to possess certificates for each isolated application and will need to be familiar with the policies of each separate PKI [ICLP97].

The Marine Corps must ensure that its software development initiatives for PKI are in compliance with open standards and protocols and the latest PKI industry standards such as X.509. Also, developers must understand the supporting infrastructure, policies, usage, and interfaces of the Marine Corps Enterprise Network, its implementation of PKI, and how it will interoperate among other services within the DoD target PKI. The Marine Corps must also coordinate closely with NSA, DISA, and NIST to ensure that vendor solutions have properly developed their standards-based solutions to achieve true compatibility, specifically with the DoD PKI.

According to the Gartner Group, "complex directory issues will not be resolved during the five-year planning horizon. Enterprises should work to minimize directory



project impact on PKI developments by opting for industry standards solutions and migrating to new architectures as necessary” [Gar99]. To accomplish this, directory services must be founded on open systems and industry standards such as X.500 and LDAP v.3. Directories based on these standards are not limited to certain operating environments and will integrate seamlessly with other COTS software designed upon the same standards [ICLP97]. These specifications are suited both for general and special purpose directory applications [ICLP97]. Note that many COTS directory products are optimized for specific applications creating possible interoperability problems [Gar99]. For instance, a directory solution developed to specifically meet the needs of a supply and logistics systems, may incorporate subtle design characteristics that lead to incompatibilities with a solution developed for organizational travel purposes or procurement.

#### **D. KEY ESCROW**

##### **1. Definition**

Key escrow is the safeguarding of keys by trusted escrow agents for enabling decryption under specified conditions [Den94]. Key escrow is designed to provide emergency data recovery capabilities that enable decryption of cipher text through a mechanism other than the normal means used by the intended recipients of the data [Den94]. Although there are subtle differences, the terms “key escrow” and “key recovery” are often used interchangeably when describing a system for assuring government access to encrypted data [Abe97].

Key recovery, key escrow and trusted third-party systems all share the essential elements that concern us for the DoD PKI. First, the purpose of a key recovery system is to provide "a mechanism, external to the primary means of encryption and decryption, by which a third party can obtain covert access to the plaintext of encrypted data" [Abe97]. Second, common to these systems is "the existence of a highly sensitive secret key (or collection of keys) that must be secured for an extended period" [Abe97]. In addition to these requirements, key recovery systems must make decryption information quickly accessible to law enforcement agencies without notice to the key owners, making the challenge of key recovery difficult and expensive [Abe97]. For the Marine Corps' purposes, key recovery systems offer the opportunity to retrieve decryption keys of Marines or civilian employees whose incapacity prevents access to information encrypted with their encryption key.

## **2. Issues**

Key recovery enables an organization to retrieve encrypted data when keys are lost, damaged, destroyed or held for ransom [Den94]. In the event a Marine is killed or incapacitated, the Marine Corps will want the ability to access any information encrypted with the Marine's private, confidentiality key as part of his or her duties. In addition to recovering data for Marine Corps operations, key escrow is also used by government officials for law enforcement and national security purposes. Key escrow involves many legal ramifications that are beyond the scope of this chapter; however, it will focus on related issues such as key control, system performance, and policy.

One of the major issues of key recovery is the ability of the organization to retain full control of its decryption keys. Organizations want to retain control of their sensitive information, but provide the ability to surrender decrypted data to law enforcement officials if Marines become the subject of a criminal investigation. Documents encrypted with Marine Corps-supplied keys may be requested as evidence for an investigation.

For the DoD's purposes, key recovery systems should be designed to escrow private keys used for confidentiality. Private keys used for authenticity (digital signature keys) will not be escrowed, since this destroys the absolute non-repudiation property that makes binding commitments possible [Abe97]. Another argument can be made that there is no justification for third-party access to signature keys that, if compromised, could be used to impersonate people, or to forge their digital signatures [Abe97]. Since signature keys can be revoked and new keys issued with the same rights and privileges as the old ones, lost private keys need not be recovered [Abe97]. Signed information will be encrypted for confidentiality with separate confidentiality keys, or might not be encrypted at all.

Other important considerations in selecting a key recovery system are performance factors such as reliability and speed of recovery. For recovering operational information, time may be a critical factor. Thus, for the Marine Corps, the time required to recover escrowed keys must be considered [Den94]. The key recovery system must be available to perform operations from anywhere in the world twenty-four hours per day. It must be reliable in the sense that escrowed keys can be recovered without flaw. The time

required to recover the key in an emergency should be minimal. Also, system cost and ease of use must be considered.

### **3. Mechanics**

The ability to retrieve backups of decryption keys under carefully defined conditions can be a critical part of certificate management [NetD99]. The recovery system itself must be secure. Due to the human element, key recovery systems are particularly vulnerable to compromise by authorized individuals who abuse or misuse their authority [Abe97]. If a key recovery agent's secrets are compromised, the damage could be catastrophic in that every escrowed key of that recovery agent would then be vulnerable to compromise [Abe97]. Thus, key recovery systems make extremely valuable targets. Policies must be written that outline administrative procedures that protect escrowed keys from compromise, loss, or abuse [Den94]. These policies must include accountability methods that link escrow agents to their actions, so individuals can be identified and held accountable for any action affecting the escrowed keys [Den94].

The significance of key recovery depends on how an organization uses its certificates. Key recovery schemes normally involve "an  $m$  of  $n$  mechanism: for example,  $m$  of  $n$  managers within an organization might have to agree, and each contribute a special code or key of their own, before a particular person's encryption key can be recovered" [NetD99]. Protection mechanisms providing security and accountability may include a combination of technical, procedural, and legal safeguards [Den94]. Some examples include auditing, separation of duties, two-person integrity, shared secret protocols for

key recovery, physical security, computer security, certification, validation and legal penalties for misuse [Den94].

The DOD PKI Roadmap addresses the need for key escrow of decryption keys. Currently, these keys must be manually escrowed by the LRA. Local policies and procedures must be developed to support this effort until an automated system is implemented by the CA's. Private keys will not be escrowed to ensure that users' digital signatures are not compromised by the recovery system. The key recovery mechanism chosen for DOD will comply with Federal Information Processing Standards (FIPS) for key recovery products [DOD99]. Forthcoming is a DoD Key Recovery policy for DoD-wide implementation [DoD99]. The policy must outline strict procedures for the recovery of lost or compromised keys to ensure that the escrow and recovery mechanisms themselves are not a means of potential compromise of the DoD PKI.

Until the Key Recovery FIPS has been published, the Marine Corps should reference preliminary criteria published by NSA to assess prospective applications providing confidentiality services [DOD99]. Although DISA is designated as the central repository for decryption keys, the Marine Corps should determine if it has a need or desire to escrow its own keys, particularly for deployed operations [DOD99]. Relying on a centralized key escrow and recovery service to recover keys compromised during combat operations may not be efficient, reliable or desirable.

Although centralization of key escrow management responsibilities results in a simpler system design, it does not provide robustness, since such a design creates a single point of failure [Abe97]. Consider that "reach back" communications from a deployed

environment to the continental Defense Information Systems Network (DISN) must compete with other priority tactical communications requirements for limited bandwidth through Standardized Tactical Entry Point (STEP) sites. Therefore, there may be periods where connectivity may be unavailable for access to escrowed keys. Another important consideration concerning the single point of failure is that if the recovery agent's private key (the key that provides access to all escrowed keys) is compromised, all recoverable decryption keys are vulnerable to exploitation [Abe97]. Various split key techniques can help mitigate the single point of failure issue with centralized key recovery systems. With a distributed key recovery system, fewer keys will be managed by a single recovery agent, helping to minimize the number of keys exposed to a corrupt recovery agent. Additionally, with a distributed system, there may be more access points through which a deployed unit can obtain access to escrowed keys.

These concerns provide strong arguments for a distributed key escrow system. Although such a distributed system may cost more to develop, operate and maintain, these costs must be weighed against the potential costs of a catastrophic compromise occurring because of a centralized key escrow system design. The total cost of ownership for a distributed key escrow system should include the cost of providing adequate protection to the distributed elements, since each component must be as strong and secure as the centralized key escrow system. These costs include hardware, software, maintenance, and personnel training.

## **E. SMART CARDS**

Security tokens may be used as a memory device to store PKI components such as private keys, digital signatures, and a user's identification information. Tokens come in many varieties to include: PCMCIA cards (or "PC" cards), smart cards, USB tokens, memory devices, and floppy disks. Each of these technologies has advantages and disadvantages. DoD's objective is to acquire token technology that provides the ability to present a digital certificate to any application on any host, regardless of platform, vendor, and application [Dre99].

The DoD is interested in smart card technology for its touted interoperability with industry, multi-application capabilities, flexibility for adding applications and software, low cost, and portability. An additional advantage to smart cards is their ability to process security information without exposing the key to the operating system as outlined in PKCS #11.

As the storage capacity and processing power on smart cards increase, other features such as biometrics may be stored on the smart card. Biometrics use physical characteristics such as fingerprints, hand geometry, or retinal scans to identify a person. Combined with a smart card and the PKI components, biometrics improve key protection, provide unique identification, and help prevent identity theft. [Dre99].

Although biometrics are unique identifiers, they are not secret. Consider that fingerprints, voice recordings or DNA can be obtained and their digital values reproduced. For example, in order to be useful as a biometric, a person's fingerprint must be stored in a database file [Sch99]. A cyber attacker will not attempt to steal the

person's finger, but will attempt to obtain the digital fingerprint that can be inserted into the target verification process [Sch99]. Biometrics work well if the verifier can verify, first, that the biometric came from the person at the time of verification, and, second, that the biometric matches the master biometric in the database [Sch99].

Another requirement for biometrics to be useful is that the connection from the reader to the verifier is secure. For example, a biometric can be used to unlock a private key stored on a smart card. Serving as a verifier, a smart card can be designed to accept and store the value of the authorized user's digital thumbprint. By placing his thumb on the smart card interface designed to capture the authorized user's thumbprint, the Marine enables the smart card to verify that the holder of the card is the Marine authorized to access the private key. In this situation biometrics serve well as a Personal Identification Number (PIN) or as a password. However, because they lack secrecy, randomness, and the ability to be updated or destroyed (characteristics normally associated with a key), biometrics are not useful when such characteristics are required [Sch99].

If smart cards are used to protect digital certificates, users will require access to card readers to conduct business. The Marine Corps must consider the costs of providing a smart card reader for each PC. Additional measures should be taken to ensure readers are acquired that are interoperable with a wide selection of smart cards rather than a single variety. Once again, the importance of a vendor-independent solution is emphasized. Current prices for readers are about \$20 or less. The Marine Corps faces the significant challenge of purchasing the necessary readers to meet the intent of the DoD PKI implementation timeline while simultaneously minimizing costs and avoiding



future incompatibilities. As readers become more common in government and industry, competition for market share should drive these products to commodity prices and implementations should become more stable, resulting in better-defined standards. The cost of replacement cards is relatively low should they be lost or stolen. In the event of loss or theft, the certificate can be revoked through CRLs and a new one issued.

Although smart cards offer these advantages, interoperability within industry is an issue. Currently there is no universal standard for all card formats. Detailed functional guidelines and specifications are needed to ensure interoperability within industry. Therefore, the Marine Corps should seek a vendor-independent solution based on extant and emerging industry standards for smart cards such as Public Key Cryptography Standards (PKCS).

## **F. CONCLUSION**

This chapter has identified multiple technical challenges and risks involved in implementing PKI for the Marine Corps. Discussing objectives and alternative solutions for addressing these challenges and risks, this chapter has argued that the Marine Corps should proceed cautiously, avoiding vendor-dependent solutions. An approach to solving PKI's technical challenges that is based on industry standards and that closely tracks DoD PKI requirements is critical to successful PKI implementation for the Marine Corps. Additionally, PKI solutions must be developed within the framework of the overall MCEN design, including the Marine Corps IA and defense-in-depth security implementations. The Marine Corps must also coordinate closely with NSA and DISA to ensure that all commercial solutions are fully compatible with the DoD PKI.

## **V. CHANGE MANAGEMENT**

### **A. INTRODUCTION**

#### **1. Purpose of Chapter**

The purpose of this chapter is to examine the potential impact of implementing PKI technologies in the Marine Corps. In developing the argument for how to create a smooth transition to a PKI-enabled enterprise network, the chapter begins with a general discussion of change, defining its meaning and importance to an organization. Next, factors influencing an organization's strategy for implementing change are presented and potential effects on the organization are described. After considering some factors influencing change, the chapter turns to a discussion of the vision for change. Alternative models illustrate the potential impact of an organization's vision for change implementation.

Turning from a general discussion of change, the appropriate change implementation model and strategic choices for enabling PKI implementation in the Marine Corps are described. Pace, scope, and publicity issues are identified with possible solutions to their challenges. Included in these solutions is the issue of gathering critical support from the Marine Corps' top leadership. Approaches for effectively communicating the Marine Corps' PKI implementation vision to top leadership for their critical support and also methods for gaining support at the grassroots are outlined.

Additionally, methods to modify the Marine Corps' culture for more rapid acceptance of PKI are described. These methods include conducting assessments with both technical experts and Marine Corps leaders on how best to implement a PKI, while

keeping in mind the unique requirements of the organization's culture and structure. Use of feedback processes and intermediate evaluations en route to mass implementation are discussed. Through compilation of lessons learned and metrics, the Marine Corps can improve the change process. The importance of pilot studies and evaluations to measure the Marine Corps' optimal rate of change for PKI implementation are considered.

Finally, potential sources of resistance and the need to anticipate challenges in educating users are examined. Anticipating resistance to the PKI implementation is a key step toward gaining user investment in the new technology. By maintaining good communications with the users and encouraging their internalization of PKI as part of the change process, Marine Corps leaders can accelerate the acceptance of a transition to PKI technologies.

## **2. Definition of Change**

### ***a) Importance of Change***

What is change and what drives it? "'Change,' in its broadest sense, is a planned or unplanned response to pressures and forces" [JIC93]. Without change, individuals and organizations cannot survive.

### ***b) Change as a Double-Edged Sword***

Due to the stresses introduced by change, some individuals and organizations do not survive. They collapse under the pressures and strain created by the turmoil of change. Thus, the forces of change are a double-edged sword [JIC93]. Talking about change is easy; making it happen without becoming a casualty of it is not.

*c) Attitude: The Force Multiplier*

A force multiplier in the change process is the attitude with which change is met.

Change is often a frightening experience to many. It may threaten the stake holder's power, position, and influence, creating panic or even hostility.

Ultimately, the pressures that provoke change can be considered obstacles or challenges, threats or opportunities. They can elicit despair or mobilize energy. The reaction depends on how an organization interprets the forces surrounding it, and what it does with them [JIC93].

Thus, in preparing the Marine Corps for changes in technology and business procedures as a result of PKI implementation, it is critical for leaders to understand the need to influence the attitudes of those who will be affected by change. Leaders should prime those to be affected and convince them of the need for change and the benefits to them for implementing the change.

**3. Developing Strategies for Change**

An important consideration for implementing change is choosing an overall strategy for how change will be introduced into an organization. Since it is unreasonable to assume that universal agreement will exist within the Marine Corps on the issues of how and when to embrace PKI technology, change leaders need to develop a strategy that includes decisions regarding the pace and scope of change, how grand its scale and how penetrating its effects within the organization. Another factor influencing the strategy for change implementation is the nature of the change. It is important to ask: Is the change to

be produced a slight refinement to the way business is currently done, or is it a radical departure from the traditional purpose and focus of the organization?

The scope and rate at which change is introduced has a direct relationship to both the amount of resistance to change and the ability to adapt to change. The more dramatic and rapid the changes to established methods, the greater the potential for panic and discontent. Therefore, it is critical to make users aware of the need for the change and receptive to its implementation, communicating its benefits in understandable terms.

Change leaders should not expect universal agreement on the need for change, its magnitude, time frame, and implications [JIC93]. A consciousness-raising campaign may be effective, however, some communities may accept the need for change faster than others [JIC93]. Although, there may be agreement for change, communities within an organization may disagree on the forces driving the change, thereby creating conflict over the goals, scope, and pace of change. In preparing a change in technology, change leaders must ensure that they are effectively communicating the vision and strategy for achieving intended goals. Effective communication is key to accelerating the acceptance of change.

Another challenge related to attitude is the organization's approach to change. As an example of this challenge, consider that some leaders may take a "zero defects" approach, requiring perfection on the first attempt to implement the new technology. In contrast, others may approach a new technology implementation with greater flexibility, accepting mistakes as part of the change management process.

In summary, leaders face multiple challenges in implementing change. Applying these ideas to the Marine Corps' transition to a PKI-enabled organization, the Marine

Corps must determine the services and capabilities that it wants a PKI-enabled enterprise network to provide. A vision of the PKI-enabled Marine Corps will help the organization develop its implementation plan and make appropriate product and service choices toward attaining the vision.

## **B. CATEGORIZING CHANGE**

### **1. The Vision for Change**

The first step toward realizing an implementation of change in an organization is developing the vision for it. Envisioning the future look and feel desired in an organization will help determine what changes are needed to attain that vision and the implementation plan to effect those changes. Determining what kind of change an organization requires is clearly vital, for the depth and complexity of implementation grow significantly as the changes increasingly impact the purpose, structure, and culture of the organization [JIC93]. To illustrate the impact of change on organizations, Linda Ackerman describes a spectrum of organizational change, ranging from the minor tweaking of processes (developmental), to an evolution of new technologies enhancing existing capabilities, and then to the radical, paradigm shift of organizational purpose (transformational) [ACK86].

#### ***a) Developmental***

The developmental approach to change involves little more than an improvement on existing processes. It is a tweaking or fine-tuning that is described as "the improvement of a skill, method or condition that for some reason does not measure up to current expectation...[thus] 'to do better than' or 'do more of' what already exists" [ACK86]. Simply doing old processes faster or cheaper with existing technology does

not involve complex change. A better description of complex change is an evolution of new technologies toward enhancing existing organizational practices. The developmental model then is not the best choice for implementing a PKI, since a PKI will introduce new procedures and capabilities that are dependent on new technology.

*b) Transitional*

A PKI implementation falls under the more difficult categories of change. Better management skills and imagination are required for changes that are far-reaching and potentially wrenching [JIC93]. The transitional approach is characterized by evolutionary changes in technology and procedures that enhance existing capabilities, but do not radically alter the core functions of the organization [JIC93].

A PKI-enabled organization is not difficult to picture. PKI enhances existing capabilities, but introduces new technologies to provide these additional enhancements. PKI thus results in a known new state. The approach to achieving this new state can be transitional: an evolutionary process requiring the "management of the interim transition state, over a controlled period of time" [ACK86]. This process may involve many transitional steps, "during which the organization is neither what it once was nor what it aims to become" [JIC93]. "Such steps [may] include temporary arrangements, pilots, [and] phased-in operations" [JIC93]. For the Marine Corps, this could involve three stages: an initial phase to register and train PKI support personnel; next, a ramp-up phase to include all users, and thus meet DOD requirements; and, finally, a sustainment phase that would involve ongoing management of the existing user population as well as admitting new Marines and civilians.

The transitional model is the optimal approach for PKI implementation for the following reasons: PKI builds upon existing procedures but introduces new technology, thus, an evolutionary process of "crawl, walk, run" can mitigate resistance to required cultural change. With a PKI, users will have to become more security conscious to appreciate the PKI's purpose and capabilities. Applications requiring a PKI will force them to use new procedures. The transitional model can help Marine Corps leaders ease the Marines into a new state of network security awareness, accelerating the acceptance rate of the PKI technology.

*c) Transformational*

In the interest of understanding cultural change, it is important to illustrate how PKI does not fit the third model, the transformational approach. The transformational model is associated with more radical changes involving the development of new beliefs or systems that alter the core function of the organization. For the Marine Corps, this can be illustrated by the adoption of beliefs that require the Marine Corps to change its warfighting focus to, say, a charity service, requiring a radical change in doctrine and training. PKI implementation will not change the core function of the Marine Corps. The implementation of PKI will build upon existing Marine Corps capabilities, resulting in a Marine Corps with enhanced network security whose organizational form is easily pictured. PKI will not radically alter the values or structure of the organization. Thus, unlike the transformational approach, a PKI implementation plan will not result in the "emergence of a new state, unknown until it takes shape, out of the remains of the chaotic death of the old state" [ACK86].



A PKI enhances current security practices through new technology. A PKI's capabilities allow the organization more flexibility to use public networks for exchanging sensitive but unclassified information. Although a PKI's procedural and technical changes will affect the organizational culture, the effect will not be akin to the life cycle of the mythical Phoenix. The Marine Corps will not suffer a violent death to be reborn into a new state.

In a transformational approach the new state is "catalyzed by a change in belief and awareness about what is possible and necessary for the organization. It is something akin to letting go of one trapeze in mid-air before a new one swings into view" [JIC93]. Transformational models are described where "the new state is usually unknown until it begins to take shape" [ACK86]. Since the new state resulting from a PKI implementation is fairly well understood, the transformational approach does not fit.

## **2. Strategic Choices for Enabling Change**

Once the decision has been made on the type of change needed (developmental, transitional, or transformational), the organization must then make strategic decisions to enable the change to be effective [JIC93]. These decisions are made prior to actual implementation of the change and address the question of how to optimally prepare the organization to accept and implement change [JIC93].

### ***a) Pace***

The first choice is pace. It defines the rate at which an organization plans and then implements its design for change. An organization should consider options for accommodating trial and error in the change process. In the case of PKI implementation,

adoption of the transitional approach does not require radical changes overnight.

Although the DoD PKI implementation schedule is tight (it requires full PKI compliance throughout DoD by October 2000), the demand for change does not preclude an experimental approach using pilot studies, user surveys, and publication of lessons learned. For example, the pace envisioned can accommodate pilot studies used to evaluate performance and collect lessons learned on the way to an organization-wide implementation.

***b) Scope***

The next strategic choice is scope. Scope is related to pace, "stemming in large measure from the vision of what change is needed" [JIC93]. The decisions for scope are influenced by questions of scalability: should the change start small and grow as understanding of procedures, benefits, and techniques for use of the new PKI grow in sophistication, or should change begin on a grand scale? A more important question is: If the Marine Corps starts with a small PKI implementation, can the system grow large? Some vendor solutions cannot. Answers to these questions will determine whether the organization begins with a pilot program or starts with the "grand design" approach.

(1) **Pilot Programs.** There are good reasons for adopting pilot programs. Through well-placed pilot programs, the Marine Corps, with its unique culture and clearly defined organizational structure, can gather lessons learned that would benefit a PKI implementation for the Marine Corps as a whole.

To use pilot programs effectively, the Marine Corps should choose a location and unit that is representative of the rest of the organization. The pilot program

should be generalizable to the rest of the organization. [JIC93]. If selection of a representative test is not carefully considered, the pilot may not be generally applicable and a Return On Investment (ROI) in the pilot program will not be realized.

(2) **Grand Scale.** For implementing a PKI on a grand scale, change leaders need to consider the impact of numerous, broad sweeping changes to the Marine Corps network security infrastructure and policies. One significant consideration is the number of changes that can be introduced into any one area before personnel become overwhelmed. If the high risk/high reward approach to simultaneously blitz an organization with a large number of consistent changes is chosen, will maximum impact and effectiveness be ensured? [JIC93]. Some of the things that must be done for implementation of either a pilot program or larger plan include the following.

(a) *Develop Training Plan.* If the grand scale implementation is chosen, a carefully planned training program will be needed to provide the Marine Corps with knowledgeable systems support personnel who understand the tactics, techniques and procedures for implementing a PKI. A pilot program's scope may not involve large numbers of personnel, so the training plan challenges may be more limited. Training programs should be examined as candidates for outsourcing.

(b) *Place PKI Support Personnel.* Related to the scope of the PKI implementation plan is the requirement for support personnel. Change leaders will need to make decisions in choosing the location of PKI support personnel throughout the Marine Corps that provides optimal user support. These decisions are related both to geography and organizational structure issues. The objective is to provide users with the

most convenient access to PKI support personnel. An effective approach may be to build PKI support offices upon the Marine Corps' clearly defined organizational structure. In determining support personnel placement for optimal effectiveness and availability, change leaders can build upon this hierarchy; however, these decisions present a significant challenge.

Solutions to this issue are influenced by existing network infrastructure capabilities and bandwidth requirements for implementing a PKI. Sufficient network infrastructure may be lacking to support user registration at every unit. Therefore, without adequate infrastructure in place, this design may not be feasible in the near term.

Since users of the PKI must be registered by a Local Registration Authority (LRA), they will need to travel to the nearest PKI registration office. Poor planning in the placement of registration facilities (LRA's) will lead to excessive travel costs and inconvenience to users, adversely affecting the acceptance rate of PKI technology.

(c) *Source of Support Personnel.*

(i) *Skills.* Related to the granularity issue of where and at what level to place support personnel is the question of core competencies required for providing PKI support. What skills and education are required to run the PKI? Will PKI support responsibilities require full-time personnel or can they be assigned to individuals as a secondary or collateral duty?

Another issue is the question of internal versus external sources of personnel? From where will these personnel be acquired? Can they be outsourced or must they come from within the organization?

(ii) Internal. The Marine Corps is currently considering options to obtain PKI support personnel from its administrative community, communications community or both, since some tasks are administrative while others are highly technical.

(iii) External. The Marine Corps should also examine the benefits of outsourcing PKI support personnel. With outsourced support, additional security questions arise. For example, what security clearance must contractors have to gain access to Marine Corps facilities? What additional clearance will be required to install, operate, and maintain the equipment required for their support? Must the work be done on a Marine Corps base or can these responsibilities be done from a remote site? What additional vulnerabilities will be introduced by outsourced services?

*c)      **Publicity***

In preparing the Marine Corps for PKI implementation, change leaders should develop a public relations strategy for communicating to stakeholders that change is coming. Important questions include "how loud, how long, and to whom should the organization announce change is on the way?" [JIC93].

(1) Hype vs. Stealth Approach. Some change leaders may argue that PKI implementation should be announced with great fanfare, bringing out buttons, billboards, T-shirts, newsletters and celebrity speakers. The rationale for this

approach is based on the argument that change requires clear symbols, messages, and motivational cues, stimulating interest and commitment at the outset of the change process [JIC93]. However, this approach may unfairly raise expectations [JIC93]. When PKI implementation becomes highly visible, change leaders are exposed to great criticism should PKI not live up to user's unrealistic expectations, inflated by overzealous public relations.

In light of this real possibility, change leaders may want to take a quiet, understated approach to announcing PKI developments to the Marine Corps. In this way change leaders can better manage resistance, allow mistakes in the learning process, and moderate expectations for the PKI implementation. Additionally, this approach permits flexible adjustments to the change management plan [JIC93].

(2) Communicating Change to Marines. The Marine Corps has a distinct advantage over other organizations when implementing change in that Marines receive orders then carry them out expeditiously. Thus, change leaders could tell Marines to use PKI-enabled applications, and they would--without question. Yet, under the circumstances the Marines would not have any idea why they should use PKI-enabled technology. It is anticipated that Marines will respond to and invest in the PKI more readily if told why it is being implemented. Change leaders should tell Marines in non-technical language what the current threats are that create a need for PKI, what protections PKI provides, and how PKI affects them.

Great gains can be realized by choosing the right representatives to lead the change to a PKI-enabled Marine Corps and explain its benefits. One effective

way to convey the vision for the PKI is to choose a spokesperson to whom Marines can relate. This person should be a top-level leader, demonstrating to Marines that the PKI is a priority initiative and driven from the highest levels. Additionally, the spokesperson should be representative of the Marine Corps' culture. Rather than having an academic or network security professional who might use technical language to explain the PKI, the Marine Corps should choose someone to whom Marines can relate. A better choice for the Marines may be the Commandant or Sergeant Major of the Marine Corps with whom they immediately identify as both an authority and a fellow Marine. Change leaders can craft the message for the spokesperson, so that it articulates the PKI vision and carefully avoids technical computer jargon. The goal of the message should be to tell Marines about the basic capabilities and protections afforded to them by the PKI. In this way, the careful choice of the spokesperson can accelerate the acceptance of PKI.

### **C. CHANGING THE CULTURE**

#### **1. Overcoming Resistance to Change**

##### ***a) Conduct Assessments: Is Change Needed?***

Since change is often painful, disruptive, and time consuming, the Marine Corps should evaluate the validity of stated requirements for implementing PKI before subjecting people to the change process. Once the articulated requirements have been validated, leaders should prepare to explain to the stakeholders why the changes are needed and what benefits will accrue from making the changes. This section offers several methods for overcoming resistance to change.

**b) *Convince Yourself First: Anticipate Resistance and Questions***

As a preparatory step toward implementing the Marine Corps PKI, leaders should anticipate resistance to change. To provide cogent counter-arguments to naysayers, change leaders need to identify the stakeholders and what they fear from change. In anticipating potential resistance, leaders must ask: Who is threatened by change and why? Will organizational power gravitate from one group to another due to the change? Can I, as a change leader, prove their fears unfounded or at least mitigate them? Arguably, the most important issue in presenting counter-arguments is believing that the change is not only necessary, but also good for the organization. As a leader of change, one must be convinced of the need for change before attempting to convince others of it [JIC93].

**c) *Identify PKI-Enabled Applications Users Require***

To help the transition to the Marine Corps PKI, change leaders should anticipate that users may accept change more readily if they have an application requiring PKI capabilities. When users have an application that they use on a daily basis that can be enhanced by a PKI, change will seem less arbitrary. For example, fitness report applications, human resource database applications, and mission-critical applications requiring authentication could benefit greatly from PKI protections. Instead of imposing change on users, management can identify applications that naturally need these protections; thus, users will ask for PKI enhancements. In this way PKI is "pulled" by the applications, not "pushed" by management.

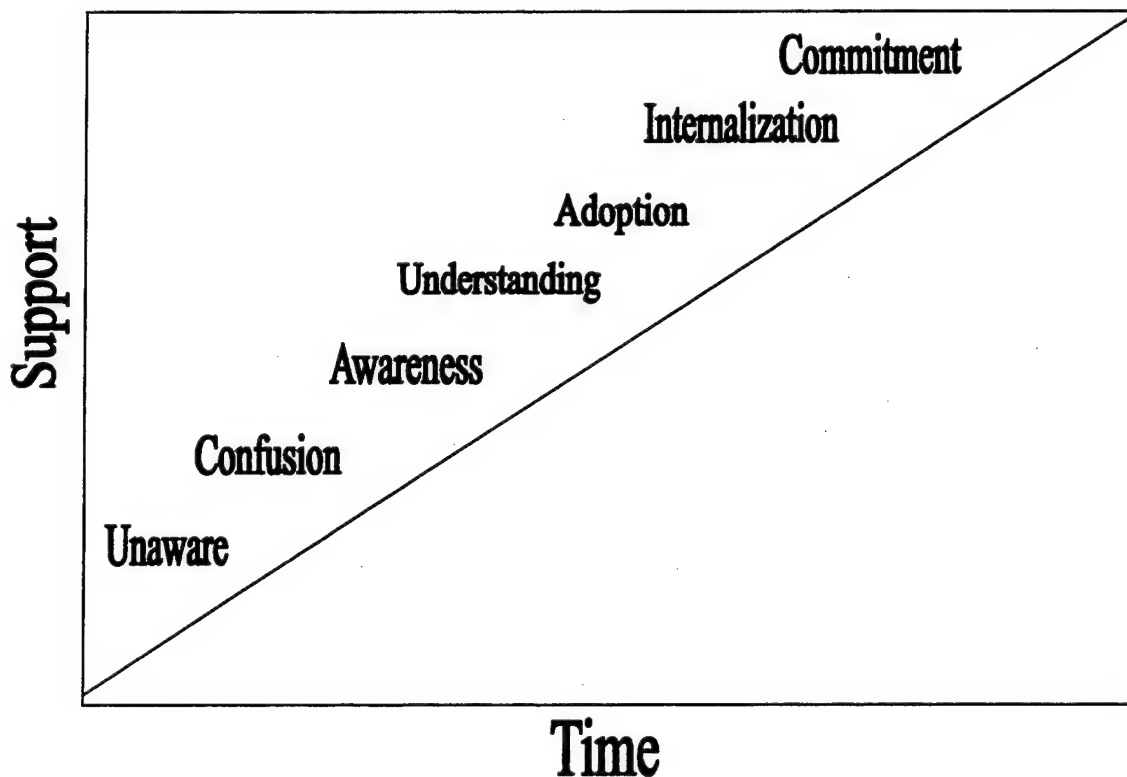


## 2. Education and Training

### a) Education

Familiarity is key to overcoming the "too hard" reaction from many frustrated users. Change leaders should strive to educate new users on the capabilities that a PKI provides and the protections it affords them. The goal of this approach is to integrate security consciousness into the Marine Corps' organizational culture such that it will affect every aspect of critical business processes. If this heightened sense of security awareness and the protections afforded by the PKI do not permeate throughout the organization, the Return On Investment (ROI) in the PKI (as well as other network security products) will not be realized.

### b) Change Adoption Model



**Figure 5-1. Progressions of Change Adoption [JIC90].** Change adoption is an evolutionary process. People involved in change implementations progress from unawareness to raised consciousness and finally commitment to the change implementation.

Figure 5-1 illustrates the progression of change adoption for an individual or organization. Although results will vary due to the nature of the change and the characteristics of the individual or organization, it can be shown that a direct relationship exists between understanding requirements for change and support for change. Simply stated: as the level of understanding of the need for change increases over time, support for change will increase [JIC90].

*c) Training*

User training should focus on the individual's responsibilities with respect to PKI technology. First, the PKI user must register with the proper authority, providing appropriate documentation. Once the user obtains his or her private key, he must protect this key from disclosure. Initially, a user's private key will be downloaded onto a diskette, so that it can be stored in a safe or locker to which only the user has access. The user must understand that the integrity of the Marine Corp's PKI rests on the fundamental principal that the user must safeguard his private key and use it for its intended purposes only.

In the future, smart cards may be used to store the private key along with other personal information, identifying and authenticating the user. This information can be read using a smart card reader when the user needs to transmit a message or complete a transaction requiring his digital signature. Users will require training on smart card storage and protection and also on use of smart card readers and smart card-enabled applications. For more on smart card technology, see Chapter IV.

Since protection of the user's private key is paramount, users must receive training on notification procedures in the event that the private key is compromised. Users must know who to inform and, to minimize potential damage, how and why to do this as soon as possible. Additionally, the user should understand that once his or her public certificate has been created and published to a directory service, anyone with access to the directory could use this certificate to exchange information securely with the user.

### **3. Centralization of Procurement**

Another step toward changing the Marine Corps' organizational culture is in the standardization and centralization of procurements for network security technology. A central procurement authority for networking security technologies would have oversight of all network security procurement initiatives, assuring interoperability and economies of scale. Using a "cheaper by the dozen" approach, the Marine Corps can reduce its costs for software and hardware maintenance and its personnel training costs. Standardization will reduce the overall number of systems supported. With fewer systems to support, the organization reduces training costs for its users and systems support personnel.

Centralization of procurement may cause long delays between the articulation of purchase requirements and the actual receipt of goods, creating a technology gap between Marine Corps PKI technology and current PKI standards used by industry. A serious drawback, this situation can lead to problems in interoperability with other services, agencies, and contractors.

To mitigate interoperability challenges in procuring network technology, the Marine Corps should develop an Enterprise Level PKI Policy, based not on vendor-dependent, application layer solutions, but on open architectural standards. Based on

standards, the policy should be crafted to support an architectural framework designed for desired services and capabilities, not vendor-dependent applications. Leveraging the capabilities of a layered, defense in depth architecture based on open standards, protocols, and specifications such as X.500, X.509, and LDAP, the Marine Corps can craft a policy for modularity, flexibility, and interoperability while providing robust security. Thus, the Marine Corps' security architectural framework can integrate both its legacy systems and a broad spectrum of standards-based COTS products. Additionally, a policy based on industry standards provides flexibility, allowing the Marine Corps to evolve its architecture to integrate emerging technology standards into the enterprise network.

Historically, the Marine Corps has selected vendor-dependent applications based not on industry standards but on basic requirements and lowest cost. This method has led to stove-piped systems developed without regard to interoperability or integration into the enterprise network. Breaking from the past, the Marine Corps should plan a PKI architecture designed not only for current needs, but also for integration with future systems. This architecture should be based firmly on industry standards and developed within the overall context of the Marine Corps' Information Assurance (IA) Plan. This is the optimal approach for the Marine Corps, enabling flexibility, interoperability and security based on standards and allowing smoother integration of emerging, standards-based applications.

The Marine Corps needs PKI architectural policies, not product-specific policies. The Marine Corps must take a proactive stance in determining what capabilities the organization wants now and in the future and design the architecture to fit these needs.

Only after designing the PKI architectural framework can the Marine Corps begin looking for applications to interoperate within this design. The Marine Corps should not rush to buy a proprietary, non-standard PKI product and attempt to redesign its architecture around it. Re-engineering an architecture around a product is usually more expensive than to engineer the desired capabilities into the architecture from the beginning. With the framework established, the Marine Corps should look for standards-based solutions that design their interfaces to specifications, so the organization can use any application that meets the specification and avoid vendor-dependent, stove-piped solutions.

Candidate COTS solutions must conform to existing security and infrastructure policies of the Marine Corps Enterprise Network (MCEN). When considering COTS products, the Marine Corps must ensure these products will integrate with existing security systems such as VPNs, firewalls, and directory access control features, so that work-arounds will not be required.

#### **D. SUMMARY**

Implementation of the Marine Corps PKI fits a transitional model, enabling a controlled, evolutionary pace for change. A transitional model will allow change leaders the opportunity to conduct pilot studies, gather metrics, and capture lessons learned. Even a smooth change transition will have many challenges, not least of which is stakeholder resistance. This chapter has described potential change management challenges resulting from the Marine Corps' implementation of PKI. Planning change in terms of the Marine Corps' unique culture and organizational structure can mitigate many of these challenges. Based on an understanding of these, this chapter has highlighted

several issues for the Marine Corps' consideration. To sustain user's investment and interest in PKI, identification of a PKI-enhanced application that will be appreciated by users is required. Building the PKI support structure into the existing Marine Corps organizational structure will reduce user resistance to change and accelerate acceptance. Finally, the Marine Corps' top leadership must embrace PKI technology and its benefits, driving the change process from the top.



## VI. CONCLUSION

The Department of Defense is working aggressively to develop and implement a layered, comprehensive, and redundant network security strategy. The defense-in-depth concept integrates numerous different, but complimentary security systems into one cohesive, structured model capable of meeting a growing variety of threats. The Marine Corps has made significant strides in developing a robust network defense by installing firewalls at each point of presence into the Marine Corps Enterprise Network, as well as intrusion detection systems and other measures to monitor traffic passing to and from its internal networks. The DoD's public key infrastructure represents a critical element of the overall defense-in-depth strategy that provides services supporting the essential security ingredients of confidentiality, authentication, integrity, and nonrepudiation. A PKI does this by providing mechanisms such as secure cryptographic key distribution and digital certificates for network identification and authentication purposes. The Marine Corps must begin to capitalize on the advantages of public key cryptography by integrating PKI elements into its existing security architecture. This thesis has established a preliminary roadmap outlining the objectives and strategies the Marine Corps should pursue in its efforts to integrate a PKI into the Marine Corps Enterprise Network.

Public key cryptography is one of the most promising security solutions to come onto the scene in a long time [Bhi98]. Through the proper development of a PKI, the DoD and Marine Corps can leverage this technology to support a number of operational



and administrative functions providing convenient and efficient transactions over the NIPRNET and Internet. However, given the complexity of the infrastructure required to support a PKI, it can be extremely challenging to deploy and maintain [Bhi98]. This thesis has provided an analysis of the challenges the Marine Corps will face in developing and implementing a PKI and has described a framework within which development efforts may proceed. The Marine Corps will need administrators who understand network security as well as developers who can build secure applications using PKI tools [Fra99]. These administrators must be able to turn the PKI into a seamless, integrated secure system capable of providing critical identification services and withstanding a variety of attacks [Fra99]. Further research needs to be conducted to determine the most efficient and cost effective source of personnel to administer a Marine Corps PKI. Options may include a mix of Marines, USMC civilian employees or contractors, and outsourced vendor support. If outsourcing is considered, which elements of the Marine Corps PKI are candidates and which are considered inherently governmental?

Implementing a standards-based solution is the key to ensuring and maintaining interoperability within the DoD and federal government, as well as with DoD contractors, foreign allies, and private industry. Although waiting for standards to solidify has traditionally been a slow process, it will eventually happen for PKI implementations, leading to interoperability between different vendors' products [Fra99]. However, as vendors aggressively compete to gain industry acceptance and market share, not all PKI products are likely to survive. The Marine Corps should actively monitor standards progress, market trends, and DoD development efforts to ensure that the Marine Corps'

solution is both consist with DoD efforts and industry standards. Any PKI solution should provide broad support for applicable existing and emerging standards for both the US government and the private sector [Des97]. This thesis has identified and described a few of the technical challenges relating to interoperability, such as directories and smart card technologies. PKI interoperability is a broad and complex topic involving several issues that should be researched in greater detail.

In addition to the topics discussed above, several other issues of related research are identified below:

- Legal issues involving public key cryptography and infrastructures, such as liability and acceptability of digital certificates. The current state of federal law presents uncertainties in relation to the formation and enforcement of electronic agreements [Bau97]. Further research may focus on the legal parameters necessary to create and enforce legal binding commitments involving digital certificates with the Marine Corps and DoD-wide PKI. What type of transactions may be conducted utilizing PKI services, what procedures must be in place to ensure the bindings necessary for electronic contracts are enforceable, what risks are involved, and how can the risks be mitigated?
- The tradeoffs of Certificate Revocation Lists vs. On-Line Certificate Verification. Certificate verification is a critical process for maintaining a high level of trust in the PKI. Scalability in relation to performance requirements is particularly important when

implementing on-line verification, a.k.a. real-time status checking. Scalability is crucial for preventing bottlenecks and providing responsive, on-line verification services. Due to the limitations of CRLs in providing current revocation information, the Marine Corps may find a need for real-time verification via server queries in addition to CRLs. Depending on the frequency with which an organization publishes its CRLs and the speed of directory replication, directory information may become obsolete. Therefore, the tradeoffs between on-line verification and CRLs should be examined in terms of bandwidth requirements, existing infrastructure and PKI policies for updating directory information.

- Integration of PKI directories with Marine Corps- or DoD-wide metadirectories. The Marine Corps will want to access directory resources throughout the DoD PKI and PKIs of allied organizations without having to develop expensive new systems. Therefore, the Marine Corps should use a common-sense approach to interoperability and look for commonality and open solutions for its certificate repositories. In this way future unions of PKIs (i.e., inter-agency and inter-service) can be formed to facilitate national, multi-national (NATO/inter-allied) and multi-organizational identification and communication solutions for the information societies of the future.

- System compromise and disaster recovery policies, procedures and mechanisms. As a DoD and Marine Corps PKI becomes fully established and utilized, PKI services will become increasingly critical to daily electronic operations. Emergency policies, procedures, and mechanisms must be in place to ensure that operations may continue in the event of a compromise or disaster. Research should be conducted on how to develop and support recovery systems to minimize the down time of any element of the PKI system, maximize the overall availability of PKI services, and continue to operate despite the loss of specific services.
- Analysis of a requirement for a Marine Corps vs. DoD key escrow and recovery mechanisms. Should the Marine Corps develop mechanisms and procedures for escrowing the confidentiality private keys of its users? Research may focus on the Marine Corps' requirements for key recovery and potential legal issues that may exist between the Marine Corps, DoD, and PKI users regarding the location of the escrow services. Does the Marine Corps need to have full control over and access to the escrowed keys of its personnel or can this task be sufficiently performed by the DoD certificate management services? Additionally, the Marine Corps should conduct an analysis on the risks of establishing a centralized key escrow system versus a distributed one. Although centralization provides easier management of keys, it

also provides a central point of failure and high value target for criminals. For any design, the total cost of ownership must be evaluated.

- *Analysis of the requirement for tactical certificate management services and Certification Authorities.* Tactical exercises, operations, and contingencies will undoubtedly demand more stringent requirements from the DoD PKI and, more specifically, the certificate management services provided by the CAs. Will permanent regionalized DoD CAs be capable of meeting tactical demands or should CAs be deployed in conjunction with tactical forces? If a CA is deployed, who will own, staff, and operate the CA? What other factors (e.g., key recovery, compromise procedures, etc...) should be considered or modified to support tactical operations?
- *Analysis of the advantages and disadvantages for establishing a Marine Corps Certification Authority.* Does the Marine Corps require its own CA or can it fully rely on the services provided by DoD operated CAs? Does the Marine Corps require a CA specifically for tactical use? What are the advantages and disadvantages of a Marine Corps-operated CA?

This thesis has also addressed the need for effective change management with in the Marine Corps to mitigate the impact of public key mechanisms and the supporting infrastructure. Educating users and gaining their acceptance of the technology is critical

for the successful implementation of a PKI for the Marine Corps. However, change management is not specifically limited to PKI implementation. Research should also be conducted on how to raise the overall security awareness of users. Marines must be continually aware of the risks and threats associated with the utilization of network resources and applications. Furthermore, a basic understanding of the security technologies employed to combat these threats may be important for users to safely use network systems, with minimal risk of information compromise. This may require a fundamental change in the attitudes or mindsets of Marines and Marine Corps employees. However, just as Marines have always understood the weapons they use to fight and win conventional wars, Marines increasingly must understand the weapons used to fight and win battles involving information warfare.



## LIST OF REFERENCES

- [Abe97] Ableson, Hal, Anderson, Ross, Bellovin, Steven M., Benaloh, Josh, Blaze, Matt, Diffie, Whitfield, Gilmore, John, Neumann, Peter G., Rivest, Ronald L., Schiller, Jeffrey I., and Schneier, Bruce, *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, [http://www.crypto.com/key\\_study/report.shtml](http://www.crypto.com/key_study/report.shtml), 1997.
- [ASD98] Assistance Secretary of Defense (C3I), *Instruction IS8500-H (Draft) Subject: Information Assurance Requirements*, December 30, 1998.
- [Bau97] Baum, Michael S., and Warwick, Ford, *Secure Electronic Commerce*, Prentice Hall PTR, Upper Saddle River, NJ, 1997.
- [Bhi98] Bhimani, Anish, All Eyes On PKI, *Information Security*, October 1998, pp. 22-31.
- [Bra97] Branchaud, Mark, *A Survey of Public Key Infrastructures*, McGill University, Montreal, 1997.
- [Cha99] Chadwick, David (1999, August), [Seminar, *X.500 and LDAP: The Complete Directory Seminar Series*, 1999], Retrieved August 22, 1999 from the World Wide Web: [http://www.techapps.co.uk/dirs\\_sem.html](http://www.techapps.co.uk/dirs_sem.html).
- [Cho94] Chokhani, Santosh, *Toward a National Public Key Infrastructure*, IEEE Communications Magazine, September, 1994, Vol. 32, Issue: 9, pp. 70-74.
- [Den94] Denning, Dorothy E., and Smid, Miles, Key Escrowing Today, *IEEE Communications Magazine*, September 1994, Vol. 32, Issue: 9, pp. 58-68.
- [Des97] Desind, B.J., Sharick, T.M., Long, J.P., Development of a Public Key Infrastructure across Multiple Enterprises, *Proceedings of the Sixth IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, June 1997, pp. 214-219.
- [Dif98] Diffie, Whitfield, *The First Ten Years of Public-Key Cryptology*, Proceedings of the IEEE, Vol. 76, NO. 5, May 1998.
- [DOD97] DISA, MITRE, and NSA, *DOD Information Infrastructure Public Key Infrastructure (PKI) Concept of Operations (Third Draft)*, 1997.
- [DOD98] Department of Defense, *X.509 Certificate Policy (Draft)*, 1998.



[DOD98a] DISA and NSA, *Functional Specification, Department of Defense (DOD) Medium Assurance Public Key Infrastructure(PKI), Version 0.3 (Draft)*, 1998.

[DOD99] DISA and NSA, *Department of Defense (DOD) Public Key Infrastructure Roadmap*, Version 2.0, 1999.

[DOD99a] Department of Defense, *Public Key Infrastructure Implementation Plan for the Department of Defense*, Version 1.0, Revision C, 1999.

[DON99] Department of the Navy Chief Information Officer, *Information Technology Standards Guidance*, Version 99-1, April 1999.

[Dre99] Dreifus, Henry (1999, July). Dreifus Associates Ltd. [Presentation, given for Department of the Navy Public Key Infrastructure (PKI) Implementation Planning Conference, July 28-29, 1999].

[DSD99] Deputy Secretary of Defense, *Memorandum Subject: Department of Defense (DoD) Public Key Infrastructure (PKI)*, 6 May 1999.

[Ent99] Entrust home page: <http://www.entrust.com>

[Feg98] Feghhi, Jalal, Feghhi, Jalil, and Williams, Peter, *Digital Certificates*, Addison-Wesley, Reading, MA, 1998.

[Fra99] Fratto, Mike, Gear Up Your PKI Pilot, *Network Computing*, July 26, 1999, pp. 38-50.

[Gar97] Garfinkel, Simson, and Spafford, Gene, *Web Security and Commerce*, O'Reilly and Associates, Sebastopol, CA, 1997.

[Gar98] Gartner Group, *Public Key Infrastructures: Trends and Directions*, Information Security Conference, Gartner Group, Inc., April 12-14, 1999.

[Gra98] Grant, Gail L., *Understanding Digital Signatures*, McGraw-Hill, Inc., New York, NY, 1998.

[How99] Howes, Tim (1999, February). LDAP: Use as Directed. *Data Communications*. [Magazine, selected stories on line]. Retrieved July 26, 1999 from the World Wide Web: <http://www.data.com/issue/990207/ldap.htm>.

[ICLM97] ICL i500 White Paper: *i500 and the Meta Directory*, Retrieved April 21, 1999 from the World Wide Web: <http://www.i500.com>.

[ICLP97] Collier, Paul (1997), ICL i500 White Paper: *i500 and PKI Solutions*. Retrieved April 21, 1999 from the World Wide Web: <http://www.i500.com>.

[Lee98] Lee, Rich, *Assessing the Business and Technical Aspects of Public Key Infrastructure Deployment*, Novell Research, <http://developer.novell.com/research/>, 1998.

[NetD99] Netscape White Paper: *Introduction to Public-Key Cryptography*. Retrieved January 21, 1999 from the World Wide Web: <http://developer.netscape.com/docs/manuals/security/pkin/contents.html>

[Sch99] Schneier, B. (1999). Biometrics: Uses and Abuses. Inside Risks 110, Communications of the ACM, vol 42, n 8, August 99.

[Shu99] Shuh, Barbara (1997, March), *Directories and X.500: An Introduction*, National Library of Canada. Retrieved July 26, 1999 from the World Wide Web: [www.nlc-bnc.ca/pubs/netnotes/notes45.htm](http://www.nlc-bnc.ca/pubs/netnotes/notes45.htm).

[Ste97] Steedman, Doug (1997). *X.500-The Directory Standard and its Applications*. [Extract]. Retrieved August 22, 1999 from the World Wide Web: <http://www.techapps.co.uk/chapx500.html>

[Web99] Retrieved July 23, 1999 from the World Wide Web: [http://webopaedia.internet.com/networks/directory\\_service.html](http://webopaedia.internet.com/networks/directory_service.html).



## BIBLIOGRAPHY

- [Ada97] Adams, Carlisle, and Lloyd, Steve, Profiles and Protocols for the Internet Public-Key Infrastructure, *Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems*, October 1997, pp. 220-224.
- [Ada98] Adamowski, Frank J., Encryption Technology Other Than PKI, *Proceedings of the 32<sup>nd</sup> Annual 1998 International Carnahan Conference on Security Technology*, October 1998, pp. 108-116.
- [Als97] Al-Salqan, Yahya Y., Cryptographic Key Recovery, *Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems*, October 1997, pp. 34-37.
- [Cla97] Clarke, Roger, and Greenleaf, Graham, *Privacy Implications of Digital Signatures*, Australian National University, Retrieved January 28, 1999 from the World Wide Web: <http://www.ana.edu.au/people/Roger.Clark/DV/DigSig.html>, 1997.
- [Cru98] Cruellas, Juan Carlos, Gallego, Isabel, Medina, Manel, and Rubia, Montse, Interoperability between X.509 and EDIFACT Public Key Structures: the DEDICA project, *Proceedings of the Ninth International Workshop on Database and Expert Systems Applications*, August 1998, pp. 661-666.
- [For98] Ford, Warwick, Public-Key Infrastructure Interoperation, *Aerospace Conference*, March 1998, pp. 329-333.
- [Hay98] Hayes, James M., The Problem with Multiple Roots in Web Browsers – Certificate Masquerading, *Proceedings of the Seventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, June 1998 pp. 306-311.
- [IETF99] PKIX Working Group, *Internet X.509 Public Key Infrastructure PKIX Roadmap (Draft)*, 23 June 1999.
- [Lai97] Lai, Chi-Sung, and Lee, Yung-Cheng, On the Key Recovery of the Key Escrow System, *Proceedings of the 13<sup>th</sup> Annual Computer Security Applications Conference*, December 1997, pp. 216-220.
- [Net99] Netscape's home page for product information:  
<http://home.netscape.com/comprod/index.html>.
- [Smi97] Smith, Richard E., *Internet Cryptograph*, Addison-Wesley, Reading, MA, 1997.

[Ste97] Steedman, Doug (1997). *X.500-The Directory Standard and its Applications*. (Extract). Retrieved August 22, 1999 from the World Wide Web:  
<http://www.techapps.co.uk/chapx500.html>

[Ver99] VeriSign home page: <http://www.verisign.com>.

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..... 2  
8725 John J. Kingman Road, Ste 0944  
Fort Belvoir, VA 22060-6218
2. Dudley Knox Library..... 2  
Naval Postgraduate School  
411 Dyer Road  
Monterey, CA93943-5101
3. Chairman, Code CS ..... 1  
Department of Computer Science  
Naval Postgraduate School  
Monterey, CA 93943-5000
4. Professor Cynthia Irvine ..... 4  
Department of Computer Science, Code CS/Ic  
Naval Postgraduate School  
Monterey, CA 93943
5. Professor Daniel Warren ..... 1  
Department of Computer Science, Code CS/Wd  
Naval Postgraduate School  
Monterey, CA 93943
6. LtCol Terrance Brady ..... 1  
Department of Systems Management  
Naval Postgraduate School  
Monterey, CA 93943
7. Maj Dan E. Morris ..... 1  
79 Whitson Ridge Dr.  
Stafford, VA 22554
8. Capt David W. Rowe ..... 1  
216 Waters Edge Dr.  
Toms River, NJ 08753

9. Assistant Chief of Staff/C4I ..... 1  
C4I Office, USMC  
2511 Jefferson Davis Highway  
Suite #2500  
Arlington, VA 22202
10. Col J.E. Vesely ..... 1  
MARCORSYSCOM  
2033 Barnett Ave Suite 315  
Quantico, VA 22134-5010
11. Col K.A. Inman ..... 1  
Director, Plans and Policy Division  
C4I Office, USMC  
2511 Jefferson Davis Highway  
Suite #2500  
Arlington, VA 22202
12. LtCol Craig Opel ..... 1  
Director, Network Operations Center  
USMC-NOC  
3255 Meyers Ave.  
Quantico, VA 22134
13. Maj John Burnette ..... 1  
USMC-NOC  
3255 Meyers Ave.  
Quantico, VA 22134
14. Capt Carl Wright ..... 1  
Security Officer  
USMC-NOC  
3255 Meyers Ave.  
Quantico, VA 22134
15. Director, Training and Education ..... 1  
MCCDC, Code C46  
1019 Elliot Rd.  
Quantico, VA 22134-5027

16. Director, Marine Corps Research Center ..... 1  
MCCDC, Code C40RC  
2040 Broadway Street  
Quantico, VA 22134-5107
17. Director, Studies and Analysis Division ..... 1  
MCCDC, Code C45  
300 Russell Road  
Quantico, VA 22134-5130
18. Mr. Paul Pitelli ..... 1  
National Security Agency  
Research and Development Building  
R2  
9800 Savage Road  
Fort Meade, MD 20755-6000
19. Capt Dan Galik ..... 1  
Space and Naval Warfare Systems Command  
PMW 161  
Building OT-1, Room1024  
4301 Pacific Highway  
San Diego, CA 92110-3127
20. Commander, Naval Security Group Command..... 1  
Naval Security Group Headquarters  
9800 Savage Road  
Suite 6585  
Fort Meade, MD 20755-6585
21. Mr. George Bieber ..... 1  
Defense Information Systems Agency  
Center for Information Systems Security  
5113 Leesburg Pike, Suite 400  
Falls Church, VA 22041-3230
22. Mr. Jim Throneberry ..... 1  
N643  
Presidential Tower 1  
2511 South Jefferson Davis Highway  
Arlington, VA 22202



23. Mr. John Mildner ..... 1  
Director of Technical Operations  
Code 72A  
SPAWAR Systems Center Charleston  
P.O. Box 190022  
North Charleston, SC 29419
24. LtCol George Whitbeck ..... 1  
MCCDC, T&E Div, DLB  
2006 Hawkins Ave.  
Quantico, VA 22134